SIGUR

Руководство администратора ПО Sigur

Редакция от 27.12.2023.

«Промавтоматика», г. Н. Новгород, 2023 г.

Оглавление

1. Введение

Данный документ содержит общие сведения о системе «Sigur», инструкцию по установке и удалению программного обеспечения системы контроля и управления доступом «Sigur», а также инструкцию по эксплуатации программы управления сервером системы.

Предприятие-изготовитель несёт ответственность за точность предоставляемой документации и при существенных модификациях в программном обеспечении обязуется предоставлять обновлённую редакцию данной документации. Данный документ соответствует версии ПО 1.6.1.9.

Последнюю версию данного документа всегда можно найти на странице.

2. Версии документа

Данный документ имеет следующую историю ревизий.

Ревизия	Дата публикации	Что изменилось
0001	05 октября 2023 г.	Версия документации, соответствующая версии ПО 1.1.1.53.
0002	11 декабря 2023 г.	Актуализация в связи с выходом версии ПО 1.6.0.1. Обновление разделов «Системные требования СКУД Sigur», «Архитектура серверного программного обеспечения», «Шифрование трафика между компонентами системы по TLS» и иных. Исправление неточностей и опечаток.
0003	27 декабря 2023 г.	Актуализация в связи с выходом версии ПО 1.6.1.9. Обновление системных требований СКУД Sigur и порядка установки ПО Sigur на Debian Linux.

3. 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.
БД	База данных.
ПК	Персональный компьютер.

4. Основные принципы работы системы «Sigur»

4.1. Обзор компонентов

СКУД «Sigur» состоит из следующих компонентов:

- **Сервер системы** – компьютер под управлением операционной системы Windows, Linux Debian или Red Hat Linux с установленным программным обеспечением СКУД «Sigur».
- **Клиентское место системы** – рабочее место пользователя системы, которое можно запустить на любом компьютере под управлением операционной системы Windows, Linux Debian или RHEL Linux, связанном с главным сервером системы по протоколу TCP/IP, или непосредственно на сервере. Количество клиентских мест в системе – неограниченно.
- **Контроллер «Sigur»** – электронное устройство, представляющее собой микропроцессорную плату высокой степени интеграции в металлическом корпусе. Контроллер подключается по Ethernet (модели с префиксом E) или к линии связи RS485 (модели с префиксом R), считывателям, датчикам и к исполнительным устройствам. Контроллер «Sigur» является сетевым контроллером с полностью автономным алгоритмом принятия решений и их регистрации. Независимо от наличия или отсутствия связи с сервером системы, контроллер принимает решение о разрешении/запрете доступа самостоятельно, на основании автономной базы ключей и режимов доступа.
  Произошедшее событие регистрируется также автономно, с указанием даты и времени встроенных часов реального времени. Все ключи, динамические временные зоны и события хранятся в энергонезависимой памяти контроллера (FLASH и FRAM).
- **Преобразователь интерфейсов USB – RS-485 «Sigur connect»** – электронный модуль в пластиковом корпусе. Обеспечивает преобразование сигналов стандартного порта USB в стандартный порт RS–485. К одному серверу можно подключить до 16 преобразователей, получая структуру линии связи типа «звезда».
  Используется для подключения к серверу системы контроллеров R-серии. Линия связи RS-485 соединяет преобразователи с контроллерами системы. К каждой линии можно подключить до 255 контроллеров. Возможно использование повторителей, увеличивающих максимальную длину линии связи в два или четыре раза.
- **Мобильный NFC-терминал «Sigur»** - любой смартфон или планшет на базе ОС Android (версии 3.0 и выше) с поддержкой NFC или OTG. Обеспечивает сбор данных о проходах людей в ситуациях, где установка стационарной точки доступа не целесообразна. События могут регистрироваться как автоматически, так и вручную оператором после предъявления пропуска терминалу или подключенному к нему внешнему считывателю. Возможно два варианта терминала — Online (терминал на постоянной связи с сервером) и Offline (автономная работа, без связи с сервером, зафиксированные события хранятся во внутренней памяти устройства до появления связи).

- **Исполнительные устройства** – турникеты, ворота, шлагбаумы или двери, оборудованные электромагнитными или электромеханическими замками. Контроллер управляет исполнительными устройствами и получает информацию об их состоянии.
- **Считыватели** – электронные устройства, предназначенные для ввода запоминаемого кода с клавиатуры либо считывания кодовой информации с ключей (идентификаторов) системы.
- **Ключ** – уникальный признак объекта доступа (сотрудника, автомобиля, посетителя). Как правило – код электронной карты.
- **Объект доступа** – сотрудник, посетитель или автомобиль, действия которых регламентируются правилами разграничения доступа.
- **Контрольный считыватель** – используется для оперативного поиска сотрудников в базе данных системы и для быстрого ввода кода нового пропуска в систему. На момент написания документации в качестве контрольных поддерживаются следующие модели: Sigur-Reader-EH (для карт форматов EM Marine и HID ProxCard II), Z2 USB (для карт форматов EM Marine, HID ProxCard II и Mifare (только в режиме чтения UID), считыватель ACR1252U (для карт Mifare) и подключение любых считывателей с выходным интерфейсом Wiegand-26 к адаптеру Sigur-Reader-W (для прочих форматов карт). Также для заведения биометрических шаблонов поддерживаются следующие модели: Biosmart FS-80 (FPS-150 – с ограничениями, возможность работы под разными ОС уточняйте у производителя), Biosmart DCR-PV, Anviz U-Bio, ВЗОР-Enroll.
- **IP-камеры** – (опционально) подразумевается установка камер около исполнительных устройств. По IP-сети могут быть подведены к серверу Sigur для цели трансляции живого видео около исполнительных устройств, а также накопления фото-архива по факту происходящих на исполнительных устройствах событий, фиксируемых на сервере СКУД. Альтернативно может быть настроена интеграция с серверами систем видеонаблюдения.
- Некоторая компьютерная периферия, (опционально) подключаемая к клиентскому месту системы:

    - **web-камеры** — для целей оперативного занесения фотографий объектов доступа;
    - **сканеры** — для цели сканирования изображений и дополнительного закрепления их к объектам доступа, для цели распознавания персональной информации при выдаче пропуска посетителю (требуется специальные лицензии);
    - **принтеры** — для целей печати информации в результате работы некоторых дополнительных функций ПО «Sigur».

4.2. Принципы работы системы «Sigur»

4.2.1. Сервер системы

Сервер СКУД «Sigur» представляет собой компьютер под управлением операционной системы Windows, Linux Debian или Red Hat Linux.

Программное обеспечение (ПО) сервера состоит из двух программных модулей:

- Сервер базы данных – предоставляет доступ компонентам системы к общей базе данных.
- Серверный модуль – обеспечивает информационный обмен с контроллерами системы по линии связи.

4.2.2. Контроллер системы

Контроллер СКУД «Sigur» является сетевым контроллером с полностью автономным алгоритмом принятия решений и их регистрации. Независимо от наличия или отсутствия связи с сервером системы, контроллер принимает решение о разрешении/запрете доступа самостоятельно, на основании автономной базы ключей и режимов доступа.

Произошедшее событие регистрируется также автономно, с указанием даты и времени встроенных часов реального времени. Все ключи, режимы и события хранятся в энергонезависимой памяти контроллера (FLASH и FRAM).

Современные схемотехнические решения и алгоритмы программирования позволили добиться следующих результатов:

- Мгновенное принятие решения контроллером о разрешении/запрете доступа. Время принятия решения не превышает 5 мс (пяти миллисекунд).
- Абсолютная независимость текущей работы контроллера от качества и наличия линии связи. При повреждении линии связи контроллер продолжает выполнять все свои функции в полном объёме (кроме функции «Зональный контроль», однозначно требующей наличия связи со всеми контроллерами системы). Случайный или умышленный вывод из строя интерфейса связи также не влияет на текущие функции контроллера.
- Гарантируется сохранность данных в энергонезависимой памяти контроллера в течение 20 лет с момента полного отключения питания.

Основные настройки, определяющие свойства подключённых датчиков, считывателей и исполнительных устройств, выполняются переключателями на плате контроллера. Текущие настройки, определяющие разграничения уровней доступа, осуществляются с помощью описываемого в данной инструкции программного обеспечения.

Все решения (о запрете или разрешении доступа, реакции на изменения состояния внешних датчиков и т.д.) контроллер принимает и регистрирует автономно, на сервер передаётся лишь информация о принятом решении.

4.2.3. Связь сервера с контроллерами

В штатном режиме сервер системы опрашивает все подключённые к нему через линии связи RS-485 контроллеры, посылая каждому контроллеру запрос о его состоянии, при необходимости передаёт дополнительные данные и получает ответ контроллера. Для IP-контроллеров постоянный опрос отсутствует, производится периодический контроль связи путём запроса к контролерам раз в 10 минут.

Работоспособность линий связи сохраняется в широком диапазоне возможных помех за счёт применяемых программных алгоритмов.

4.3. Ключевые элементы базы системы «Sigur»

4.3.1. Список точек доступа СКУД с их настройками

В списке содержатся все подключённые к системе точки доступа с индивидуальными настройками для каждой точки.

4.3.2. Список объектов доступа и пользователей системы

Список построен в виде иерархической (древовидной) структуры вложенных друг в друга отделов. Допускается любая степень вложенности отделов.

Элементы списка бывают двух видов:

1. Отделы, в которые возможно вложение других отделов и объектов доступа.
2. Непосредственно объекты доступа (сотрудники, автомобили, пропуска посетителей).

Каждому объекту доступа присваивается ключ – номер пропуска, согласно которому он идентифицируется системой при осуществлении доступа, а также режим, определяющий интервалы разрешения доступа и рабочие графики.

В этом списке также хранятся пользователи (операторы) системы, настройки их прав доступа к различным функциям СКУД.

4.3.3. Список режимов

Список содержит все режимы, существующие в СКУД. Режимы предназначены для указания правил доступа, интервалов рабочего времени а также режимов автономной работы ТД. Режим представляет собой последовательность дней заданной длины (от 1 до 32 дней) с определённой датой начала отсчёта.

В каждом режиме возможно задание дополнительных правил, определяющих логику доступа (требование санкции охраны и пр.)

Существуют четыре вида режимов:

- уровень 1;
- уровень 2;
- уровень 3;
- уровень 4.

Режимы перечислены в порядке усиления приоритета.

Каждому объекту доступа можно присвоить один режим уровня 1 и произвольное количество режимов более высокого уровня (2..4).

Режимы уровней 2, 3 и 4 введены для корректной работы СКУД в ситуациях, когда требуется гибкое временное изменение основного режима. Они имеют приоритет над основным режимом (режимом уровня 1).

4.4. Санкционирование доступа и регистрация событий системы

4.4.1. Принятие решения о санкционировании доступа

Решение о разрешении или запрете доступа принимается контроллером автономно на основании следующих критериев:

1. Наличие допуска на данную точку доступа.
2. Наличие разрешения на допуск в текущее время.
3. Наличие разрешения на допуск в нужном направлении.
4. Наличие дополнительных проверок для объекта доступа.

Результат принятого контроллером решения можно увидеть на вкладке «Наблюдение». В системе могут быть включены функции, требующие дополнительного участия сервера в принятии решения, например, функция глобального контроля повторных проходов или списание условных средств с расчётного счёта объекта доступа при проходе через точки доступа.

4.4.2. Регистрация событий системы

События системы – это разрешённые или запрещённые попытки прохода или проезда через точку доступа, факты изменения (потери или появления) связи с контроллерами и пр. События доступа регистрируются контроллером «Sigur» автономно и независимо от наличия связи с сервером, время и дата события регистрируются в соответствии со встроенными часами реального времени.

Все зарегистрированные события хранятся в энергонезависимой памяти контроллера и автоматически передаются на сервер СКУД при наличии связи.

Таким образом, в базе данных сервера хранятся все события СКУД, по которым можно получать отчёты за заданные промежутки времени.

Система хранит всю информацию о зарегистрированных ею событиях, начиная с момента её первого запуска, без временных ограничений. Количество событий в системе – неограниченно.

5. Системные требования СКУД «Sigur»

Обратите внимание, что при работе «Sigur» с функциями видеонаблюдения (трансляцией живого видео в наблюдении, записью стоп-кадров по событию и пр.) конфигурации сервера и клиентских мест будут также определяться требованиями систем видеонаблюдения и могут существенно отличаться в сторону большей мощности.

5.1. Рекомендуемая конфигурация сервера

- ОС: Windows 10 / Windows Server 2019 / Linux Debian 11 (32-разрядные / 64-разрядные) / RHEL (не ниже 9 версии с последним пакетом обновлений, только x86_64).
- Процессор: уровня Intel Core i7 и выше (8 ядер).
- Память: не менее 16 Гб.
- Свободное место на жёстком диске: 5 Гб плюс место под базу данных.
- При использовании MariaDB в качестве сервера базы данных на ОС Linux: MariaDB версии 10.3.24 и выше.
- Источник бесперебойного питания.
- Разрешение монитора: не менее 1280*1024.
- Высокоскоростной жёсткий диск (SSD или RAID-массив).
- Не менее одного свободного USB-порта (при наличии HASP-ключа аппаратной защиты).

5.2. Минимальная конфигурация сервера

- ОС: не ниже Windows 10 / Windows Server 2016 / Linux Debian 10 (32-разрядные / 64-разрядные) / RHEL (не ниже 8 версии с последним пакетом обновлений, только x86_64).
- Процессор: не менее 1,5 ГГц, 4 ядра.
- Память: не менее 8 Гб.
- Свободное место на жёстком диске: 5 Гб для инсталляции системы, плюс место под базу данных. Размер БД зависит от количества сотрудников, размера их фотографий и времени работы системы, т.к. со временем накапливается информация о событиях системы, новых режимах доступа и т.д.
- При использовании MariaDB в качестве сервера базы данных на ОС Linux: MariaDB версии 10.3.24 и выше.
- Не менее одного свободного USB-порта (при наличии HASP-ключа аппаратной защиты).
- Источник бесперебойного питания.
- Разрешение монитора: не менее 1280*1024.
- При работе с большими БД (десятки миллионов проходов и более) – высокоскоростной жёсткий диск (SSD или RAID-массив).

Дополнительные требования при использовании встроенной в Sigur функции распознавания лиц:

- Процессор: уровня Intel Core i5 и выше.
- Память: не менее 8 ГБ (в моменты максимальной нагрузки серверный процесс Sigur занимает не более 4 ГБ).

Примечание: Работа функции распознавания лиц требует уже более заметных мощностей от сервера. В качестве примера: обработка одного кадра на одном ядре Intel Core i5-7260U@2.2GHz занимает порядка 150 мс (т. е. около 26-ти кадров в секунду на 4-х ядерном процессоре). Однако, данная цифра варьируется в зависимости от размера кадра, модели процессора и многих других параметров.

Сервером СКУД, установленным на компьютер под управлением ОС RHEL, на текущий момент не поддерживается функционал встроенного распознавание лиц Sigur.
Возможность поддержки работы интеграций с оборудованием и ПО сторонних производителей (Biosmart, Hikvision, Beward, Domination), реализованных со стороны Sigur, необходимо предварительно уточнять у технической поддержки (support@sigur.com).

5.3. Конфигурация клиентского места

- ОС: не ниже Windows 7 SP1 / Linux Debian 8 (32-разрядные / 64-разрядные) / RHEL (не ниже 7 версии с последним пакетом обновлений, только x86_64).
- Процессор: не менее 1 ГГц.
- Память: не менее 2 Гб.
- Свободное место на жёстком диске: не менее 500 Мб для инсталляции системы.
- Разрешение монитора: не менее 1280*1024.

Возможна установка клиентского и серверного ПО на один компьютер, при этом следует руководствоваться рекомендуемой конфигурацией для сервера.

5.4. Требования к операционной системе

Установка сервера и клиентов ПО «Sigur» производится на компьютеры под управлением операционной системы Windows (как 32, так и 64-битной): Windows 10, Windows Server 2016 и более новых, а также Linux Debian (как 32, так и 64-битной) и RHEL (архитектура только x86_64).

Возможны произвольные комбинации сервера и рабочих мест под управлением разных ОС (например, сервер на Linux, часть клиентов — также на Linux, а другая часть — на Windows).
Независимо от типа используемой операционной системы, необходима

установка на неё последних обновлений, выпущенных производителем ОС – компанией Microsoft.

Сервером СКУД, установленным на компьютер под управлением ОС RHEL, на текущий момент не поддерживается функционал встроенного распознавания лиц Sigur.
Возможность поддержки работы интеграций с оборудованием и ПО сторонних производителей (Biosmart, Hikvision, Beward, Domination и др.), реализованных со стороны Sigur, необходимо предварительно уточнять у технической поддержки (support@sigur.com).

6. Архитектура серверного программного обеспечения

6.1. Архитектура серверного программного обеспечения

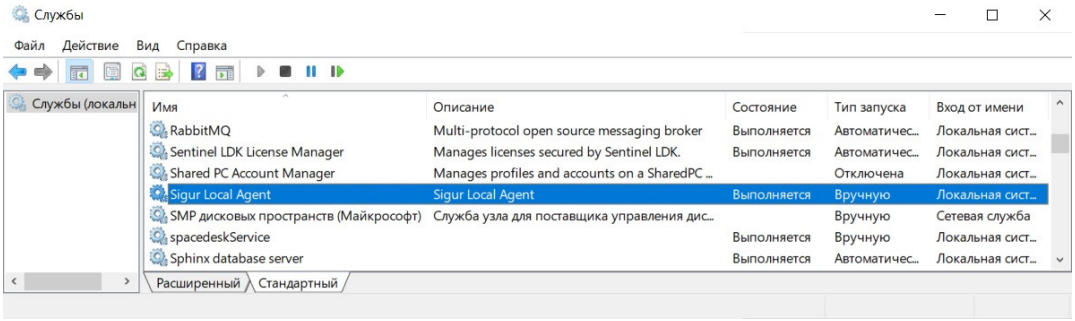
Серверное программное обеспечение состоит из сервера базы данных и серверного модуля системы «Sigur».

Сервер базы данных предоставляет доступ компонентам системы к общей базе данных.

Серверный модуль обеспечивает информационный обмен с контроллерами системы по линии связи.

В случае сервера, установленного на компьютер под управлением ОС Windows, при установке серверного ПО системы компоненты сервера регистрируются как службы (сервисы) Windows и запускаются автоматически при загрузке операционной системы.

Для управления компонентами сервера, как правило, используется программа «Управления сервером», возможности которой описаны в данном руководстве. Также может быть использована стандартная утилита Windows «Службы». Название служб, используемых системой: «Sphinx database server» , «Sigur Local Agent», «RabbitMQ».



Управление серверными процессами системы с помощью утилиты «Службы».

Когда сервер системы «Sigur» запущен, то в системе работают следующие процессы:

- «mysqld.exe», являющийся сервером БД;
- «sphinxd.exe», являющийся серверным модулем системы «Sigur»;
- «local-agent.exe», являющийся программой, контролирующей работу процессов сервера;
- процессы OpenJDK, отвечающие за работу веб-сервисов системы.

7. Программное обеспечение системы «Sigur»

Программное обеспечение (ПО) системы «Sigur» построено на основе клиент–серверной архитектуры.

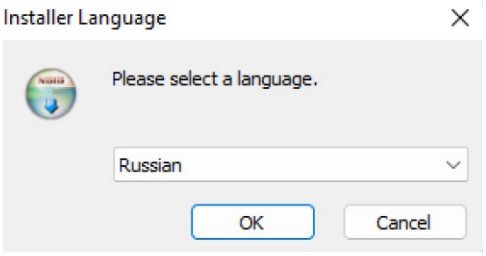
Программное обеспечение сервера состоит из двух программных компонентов. Сервер базы данных (БД) предоставляет доступ всем программным компонентам системы к общей базе данных. Серверный модуль обеспечивает информационный обмен с контроллерами системы по линии связи, а также информационный обмен сервера с клиентскими местами. Для нормальной работы системы оба компонента должны быть запущены. Управление этими модулями осуществляется с помощью программы «Управление сервером».

Программное обеспечение клиентской части состоит из программы «Клиент», которую можно устанавливать на любой компьютер, соединённый с сервером сетью по протоколу TCP. Также возможна установка клиентского ПО непосредственно на сервер СКУД «Sigur».

7.1. Установка системы «Sigur»

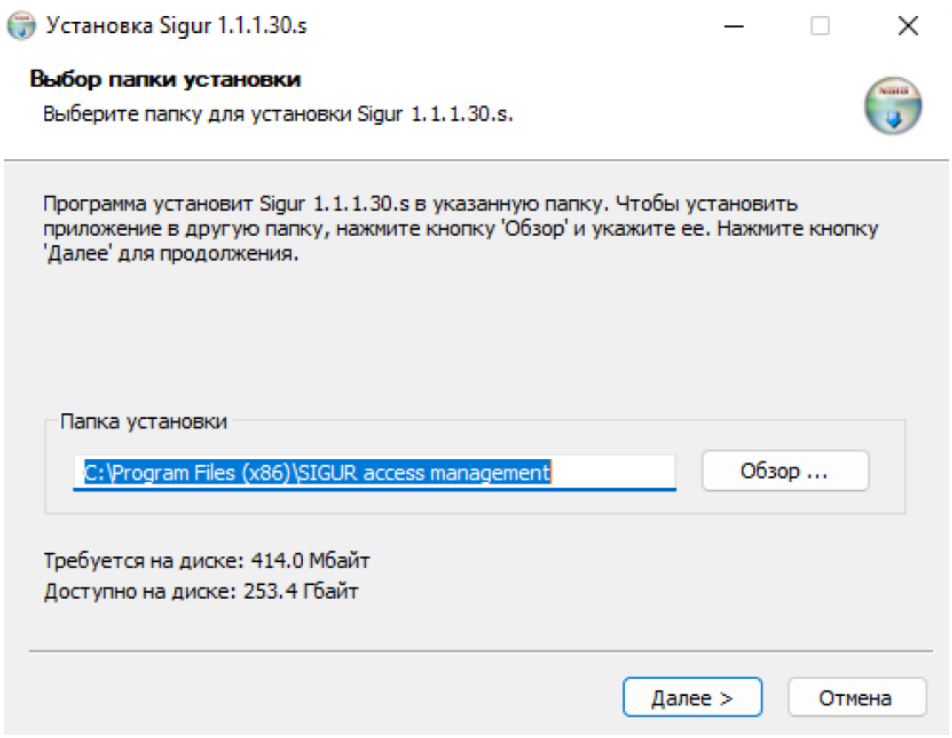
7.1.1. ОС Windows

Для установки программного обеспечения системы «Sigur» нужно войти в систему с правами администратора и запустить файл setup-XX.exe (где XX – номер версии устанавливаемого ПО).
По порядку будут следовать окна выбора языка системы:



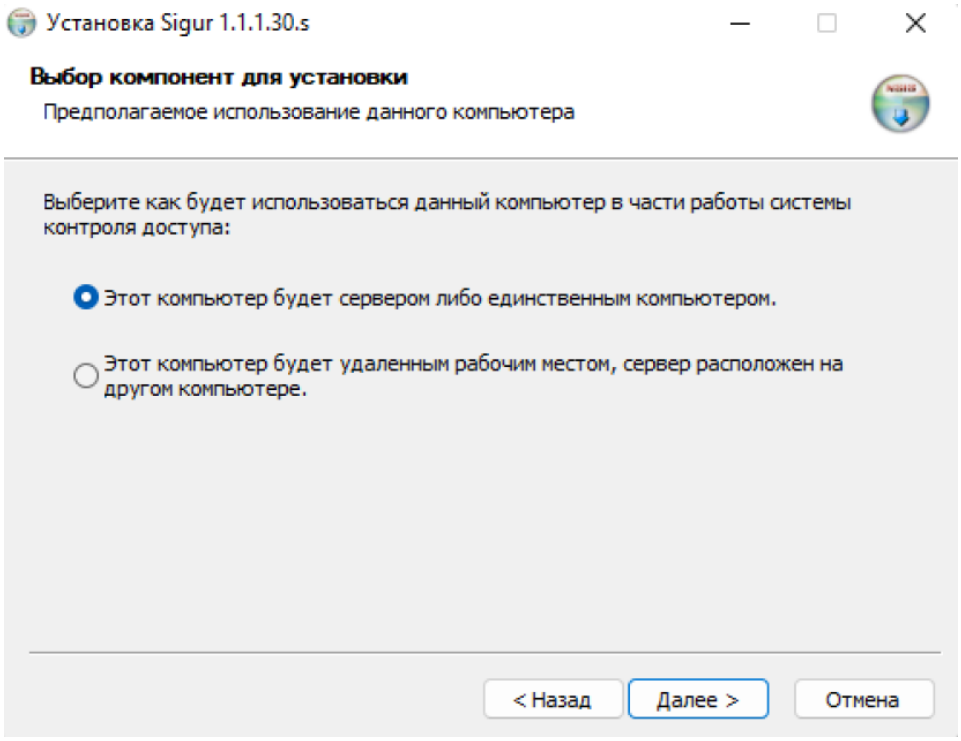
Выбор языка диалога установки.

Выбор папки для установки программы. По умолчанию программа устанавливается в папку «C:\Program Files (x86)\SIGUR access management» или «C:\Program Files\SIGUR access management», в зависимости от разрядности операционной системы. При необходимости можно изменить папку установки, нажав кнопку «Обзор».



Выбор папки программы.

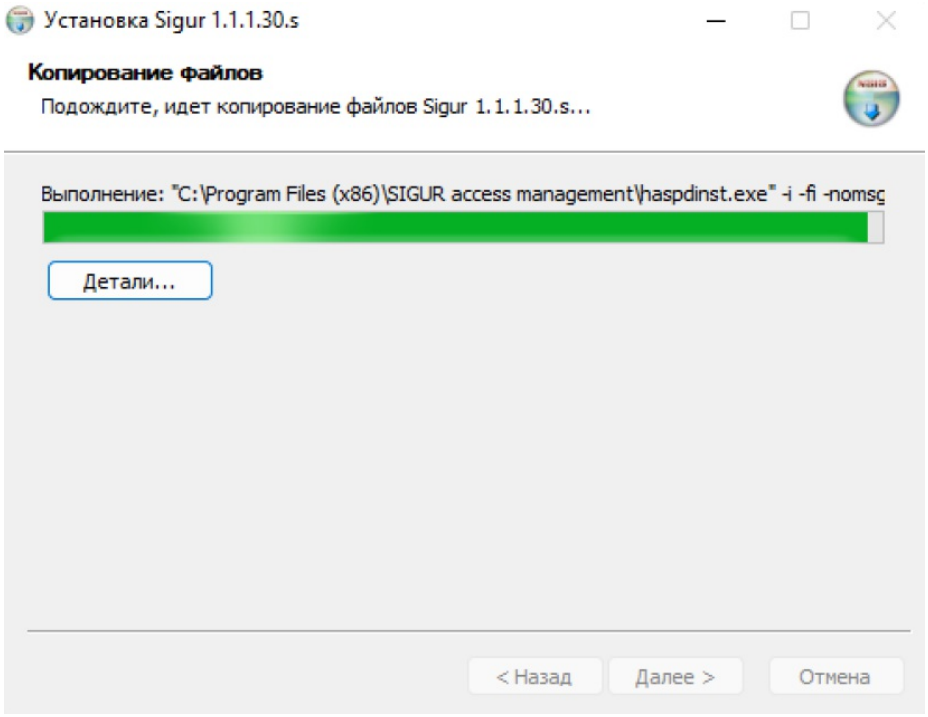
Выбор типа установки. Отметьте нужный вариант и нажмите «Далее».



Выбор типа установки.

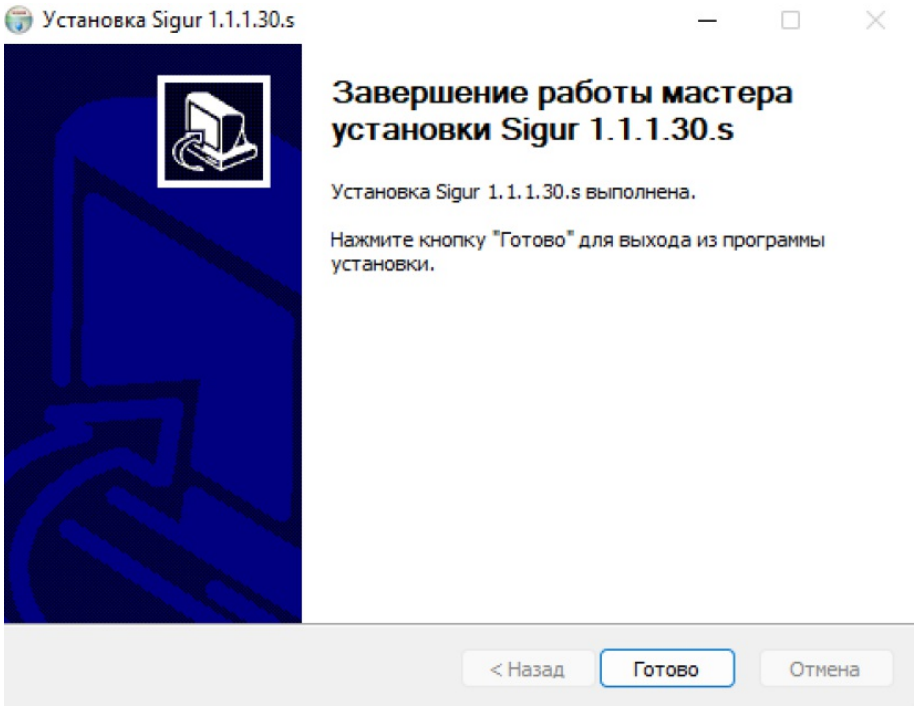
После нажатия кнопки «Установить» откроется окно «Копирование файлов», в

котором будет отображаться процесс установки программы.



Процесс установки.

По окончании процесса появится окно «Завершение работы мастера установки», в котором нужно нажать кнопку «Готово». Установка программы успешно завершена.



Завершение работы мастера установки.

При необходимости проведения «тихой» установки/обновления администраторами компании может быть использован ключ инсталлятора /S.

7.1.2. ОС Linux Debian

Обращаем ваше внимание, что установка ПО на Linux требует определённых технических навыков администрирования данной системы.

В случае ОС Linux, основанных на Debian, системой «Sigur» поддерживаются архитектуры i386 и amd64.

Порядок установки ПО на сервер системы:

1. Установите Java JRE 8 или более новую версию. Это можно сделать, например, следующей командой:

   sudo apt-get update && sudo apt-get install default-jre

   Скачать JRE также можно с официального сайта Oracle.
   Проверить версию Java можно командой:

   java -version

2. Скачайте и установите пакет клиента СКУД и все его зависимости (пакет spnxclient). Актуальные версии пакетов можно найти на соответствующей странице сайта.

   sudo dpkg -i spnxclient_*all.deb

3. Если будет использоваться HASP ключ, то необходимо установить драйвер HASP (Sentinel LDK and Sentinel HASP Run-time Environment DEB Installer for Linux).
   Распакуйте архив со скачанным драйвером и установите его:

   tar -zxf Sentinel_LDK_Linux_Run-time_Installer_script.tar.gz && cd Sentinel_LDK_Linux_Run-time_Installer_script
   tar -zxf $(find . -maxdepth 1 -name "aksusbd.tar.gz" -type f)*
   cd aksusbd/*
   sudo ./dinst

4. Скачайте и установите пакет сервера СКУД и все его зависимости (пакет spnxserver). Актуальные версии пакетов можно найти на соответствующей странице сайта.

   sudo dpkg -i spnxserver_*.deb

5. Скачайте и установите пакет веб-сервисов СКУД и все его зависимости (пакет deb-installer). Актуальные версии пакетов можно найти на соответствующей странице сайта. Пакет обязателен к установке на ПК, где будет развёрнут сервер СКУД.

   sudo dpkg -i deb-installer_*.deb

6. Установите сервер БД (MariaDB):

   sudo apt-get install mariadb-server

7. Создайте на сервере БД пользователя, от имени которого будет работать сервер СКУД. Предоставьте ему полные права на базы TC-DB-MAIN и TC-DB-LOG.
   Например, так создаётся пользователь «sigur» с паролем «my_password»:

   # mysql
   Welcome to the MariaDB monitor. Commands end with ; or \g.
   Your MariaDB connection id is 2
   Server version: 10.1.26-MariaDB-0+deb9u1 Debian 9.1

   Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

   Type "help;" or "\h" for help. Type "\c" to clear the current input statement.

   MariaDB [(none)]> GRANT ALL PRIVILEGES ON `TC-DB-MAIN`. TO "sigur" IDENTIFIED BY "my_password";*
   Query OK, 0 rows affected (0.00 sec)

   *MariaDB [(none)]> GRANT ALL PRIVILEGES ON *.* TO 'sigur'@'%';*
   Query OK, 0 rows affected (0.00 sec)

   MariaDB [(none)]> FLUSH PRIVILEGES;
   Query OK, 0 rows affected (0.00 sec)

8. Если планируется подключаться к серверу клиентами удаленно, то разрешите подключения с других хостов в настройках сервера БД.
   На современных версиях mariadb это можно сделать, отредактировав параметр «bind-address». Найдите данный текстовый параметр в одном из файлов конфигурации папки /etc/mysql/*
   Имя файла может отличаться в зависимости от системы, версии сборки сервера БД и т.п.
   Как пример, он может содержаться в файле /etc/mysql/mariadb.conf.d/50-server.cnf в блоке параметров [mysqld].
   Выставите значение параметра равным:

   bind-address=0.0.0.0

   После этого перезагрузите сервер mariadb командой *sudo systemctl restart mariadb* или *sudo service mysql restart.*

9. Для корректной работы сервисов системы необходимо отключить чувствительность к регистру в настройках сервера БД. Для этого в том же файле конфигурации (см. пункт 7) под блоком параметров [mysqld] добавьте строку:

   lower_case_table_names=1

10. Если на этом компьютере планируется использовать настольный считыватель ACR1252U, то необходимо:

    1. Установить pcscd и библиотеки к ней. Это можно сделать командой:

       sudo apt-get install pcscd
       sudo systemctl enable pcscd
       sudo systemctl start pcscd

    2. Установить драйвер считывателя ACR1252U. Архив с драйверами можно скачать с официального сайта производителя.
       Архив содержит драйвера для разных дистрибутивов и для разных архитектур. Найдите драйвер для своей системы и установите.
       Пример как это сделать для Ubuntu 18.04 (Bionic Beaver) amd64:

       wget "https://www.acs.com.hk/download-driver-unified/11929/ACS-Unified-PKG-Lnx-118-P.zip"
       unzip ACS-Unified-PKG-Lnx-118-P.zip
       sudo dpkg -i ACS-Unified-PKG-Lnx-118-P/ubuntu/bionic/libacsccid1_1.1.8-1~ubuntu18.04.1_amd64.deb

11. Запустите графическую утилиту «Управление сервером» из меню окружения вашего рабочего стола или командой:

    sudo spnxadmin

    Во вкладке «База данных» нажмите кнопку «Параметры». Далее введите параметры подключения к серверу БД (адрес, порт, имя пользователя БД и пароль). Сохраните настройки, закройте окно, после чего на вкладке «База данных» нажмите кнопку «Сброс/Создание базы». Убедитесь, что процесс создания БД не сопровождался ошибками.
    Вернитесь в окно настроек параметров подключения к серверу БД и нажмите «Тест подключения». Убедитесь, что тест завершился успешно. В противном случае проверьте реквизиты подключения к БД.

12. На вкладке «Состояние» нажмите кнопку «Старт».

13. Для запуска программы «Клиент» можно воспользоваться следующей командой:

    spnxclient

7.1.3. ОС Red Hat Linux

Обращаем ваше внимание, что установка ПО на Linux требует определённых технических навыков администрирования данной системы.

Работа ПО тестировалась и гарантированно поддерживается на следующих системах:

- Red Hat Enterprise Linux (RHEL, не ниже 7 версии с последним пакетом обновлений);
- CentOS не ниже 7 версии;
- Fedora, не ниже 20 версии.

Поддерживаемая архитектура - только x86_64.

Процедура установки ПО

1. Установите Java JRE 8 или более новую версию. Это можно сделать, например, следующей командой:

   sudo yum update java-latest-openjdk && sudo yum install java-latest-openjdk

   Проверить версию Java можно командой:

   java -version

2. Установите ПО Sigur.
   Предоставляемые пакеты:

   - **spnxclient** - пакет клиента, не содержащий библиотек для настольных считывателей. Для работы нужна только JRE (java) не ниже 8 версии.
   - **spnxclient-libs** - опциональный пакет с библиотеками клиента для работы с настольными считывателями ACR 1252U, Sigur Reader EH и другими через PC/SC. Данный пакет не является обязательным к установке. Например, его можно не ставить на сервер, если клиентское рабочее место не будет использоваться для работы с настольными считывателями. Зависит от пакета **spnxclient**.
   - **spnxserver**- пакет сервера. Зависит от пакета **spnxclient**.

   Скачать упомянутые .rpm пакеты можно на соответствующей странице сайта.
   Пример команды для установки всех компонент (клиент, сервер, библиотеки):

   $ sudo rpm -i spnxclient-x.x.x.x-0.noarch.el7.rpm spnxclient-libs-x.x.x.x-0.el7.x86_64.rpm spnxserver-x.x.x.x-0.el7.x86_64.rpm
   где x.x.x.x - версия пакета, например "1.1.1.35".

3. Установите сервер БД (MariaDB):

   sudo yum install mariadb-server

   Запустите сервер БД с помощью команды:

   systemctl start mariadb

4. Создайте на сервере БД пользователя, от имени которого будет работать сервер СКУД. Дайте ему полные права на базы TC-DBMAIN и TC-DB-LOG. Например, так создаётся пользователь "sigur" с паролем "my_password":

   # mysql
   Welcome to the MariaDB monitor. Commands end with ; or \g.
   Your MariaDB connection id is 3
   Server version: 10.5.18-MariaDB MariaDB Server

   Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

   Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

   MariaDB [(none)]> GRANT ALL PRIVILEGES ON `TC-DB-MAIN`. TO 'sigur' IDENTIFIED BY 'my_password';*
   Query OK, 0 rows affected (0.00 sec)

   MariaDB [(none)]> GRANT ALL PRIVILEGES ON `TC-DB-LOG`. TO 'sigur';*
   Query OK, 0 rows affected (0.00 sec)

   MariaDB [(none)]> FLUSH PRIVILEGES;
   Query OK, 0 rows affected (0.00 sec)

5. Если планируется подключаться к серверу клиентами удаленно, то необходимо разрешить подключения с других хостов в настройках сервера БД.
   На современных версиях MariaDB это можно сделать, отредактировав параметр "bind-address". Найдите данный текстовый параметр в одном из файлов конфигурации папки /etc/mysql/*.
   Имя файла может отличаться в зависимости от системы, версии сборки сервера БД и т.п.
   Как пример, он может содержаться в файле /etc/my.cnf.d/mariadb-server.cnf в блоке параметров [mysqld].
   Выставите значение параметра равным:

   bind-address=0.0.0.0

   После этого перезагрузите сервер mysql командой *sudo systemctl restart mariadb* или *sudo service mysql restart.*
6. Если планируется переносить БД с Windows-сервера СКУД, то необходимо отключить чувствительность к регистру в настройках сервера БД.
   Для этого в файле в том же файле конфигурации (см. пункт 5) под блоком

параметров [mysqld] добавьте строку:

lower_case_table_names=1

После этого перезагрузите сервер mysql командой *sudo systemctl restart mariadb*.

7. Если в клиентском ПО планируется использовать настольный считыватель ACR1252U, то необходимо:

    1. Установить pcscd и библиотеки к ней. Это можно сделать командами:

        sudo yum install pcsc-lite
        sudo systemctl enable pcscd
        sudo systemctl start pcscd

    2. Установить драйвер считывателя ACR1252U либо из репозитория дистрибутива следующей командой:

        sudo yum install pcsc-lite-acsccid

        Либо с официального сайта производителя. Архив содержит драйвера для разных дистрибутивов и для разных архитектур. Найдите драйвер для своей системы и установите его.
        Пример, как это сделать для Fedora Linux 36 (Server Edition):

        wget 'https://www.acs.com.hk/download-driver-unified/11929/ACSUnified-PKG-Lnx-118-P.zip'
        unzip ACS-Unified-PKG-Lnx-118-P.zip
        dnf install ACS-Unified-PKG-Lnx-118-P/fedora/31/pcsc-lite-acsccid-1.1.8-1.fc31.x86_64.rpm

8. Запустите графическую утилиту «Управление сервером» из меню окружения вашего рабочего стола или командой:

    sudo spnxadmin

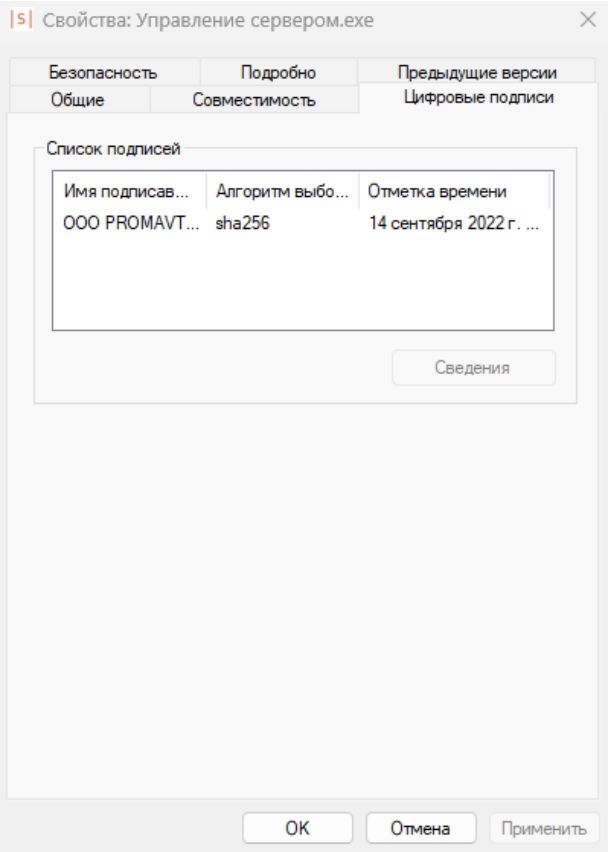
    Во вкладке «База данных» нажмите кнопку «Параметры». Далее введите параметры подключения к серверу БД (адрес, порт, имя пользователя БД и пароль). Сохраните настройки, закройте окно, после чего на вкладке «База данных» нажмите кнопку «Сброс/Создание базы». Убедитесь, что процесс создания БД не сопровождался ошибками.
    Вернитесь в окно настроек параметров подключения к серверу БД и нажмите «Тест подключения». Убедитесь, что тест завершился успешно. В противном случае проверьте реквизиты подключения к БД.
9. На вкладке «Состояние» нажмите кнопку «Старт».
10. Для запуска программы «Клиент» можно воспользоваться следующей командой:

    spnxclient

7.1.4. Проверка подлинности (цифровой подписи)

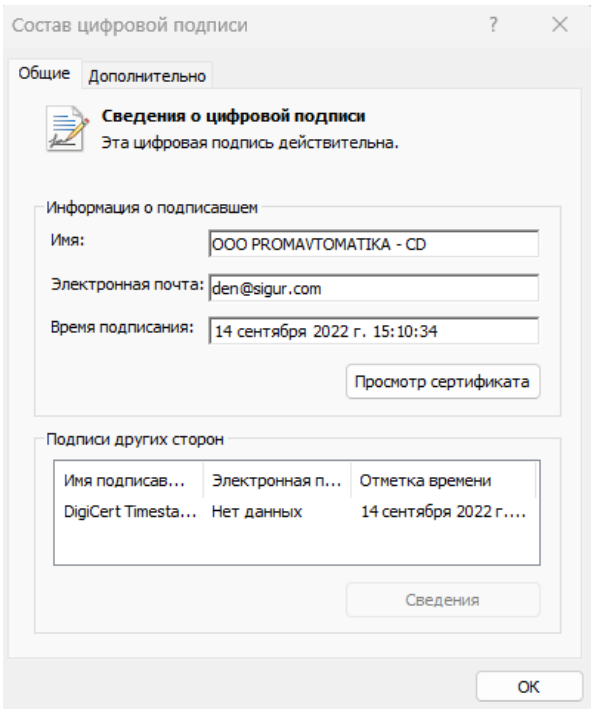
ПО Sigur имеет цифровую подпись. Проверку цифровой подписи скачанного инсталлятора и/или уже установленных исполняемых файлов (.exe) можно выполнить разными способами, в том числе самым простым - через Проводник Windows.

- Кликните правой кнопкой мыши по файлу инсталлятора (setup-XX.exe) или по исполняемому файлу программы («Управление сервером», «Клиент») и выберите в контекстном меню раздел «Свойства».
- В окне «Свойства» выберите вкладку «Цифровые подписи»:



Вкладка «Цифровые подписи».

- В списке подписей должны быть одна строка с «Именем подписавшего» - «ООО PROMAVTOMATIKA - CD». По нажатию кнопки «Сведения» откроется окно с более полной и дополнительной информацией о подписи:



Состав цифровой подписи.

Если имя подписавшего не совпадает с «PROMYSHLENNAYA AVTOMATIKA-KONTROL DOSTUPA, ООО» или «ООО PROMAVTOMATIKA - CD», то скачанный файл не является валидным файлом ПО Sigur!

7.2. Установка драйверов преобразователя USB-RS485

При использовании в составе СКУД контроллеров с интерфейсом RS485 к серверу подключается от 1 до 16 преобразователей интерфейсов USB-RS485 «Sigur Connect». Установка драйверов преобразователя подробно описана в документации на преобразователь «Sigur Connect».

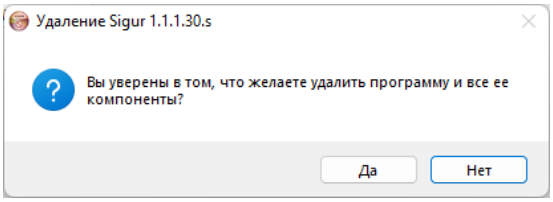
7.3. Удаление системы «Sigur»

ОС Windows

Удаление программного обеспечения СКУД «Sigur» производится двумя способами: ярлыком, находящимся в меню «Пуск» или с помощью «Панели управления».
Например, для Windows 10 это будут:

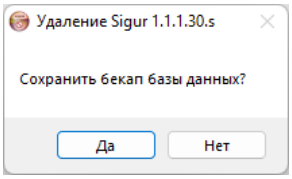
- Меню «Пуск» – «СКУД Sigur» – «Удаление программы».
- «Панель управления» – «Установка и удаление программ» – кнопка «Заменить/удалить» в строке «Sigur XX» (где XX – номер версии установленного ПО).

Откроется окно, позволяющее подтвердить или отказаться от удаления нажатием кнопки «Да» или «Нет».



Запрос удаления программы.

При нажатии кнопки «Да» откроется окно с предложением сохранить базу данных.

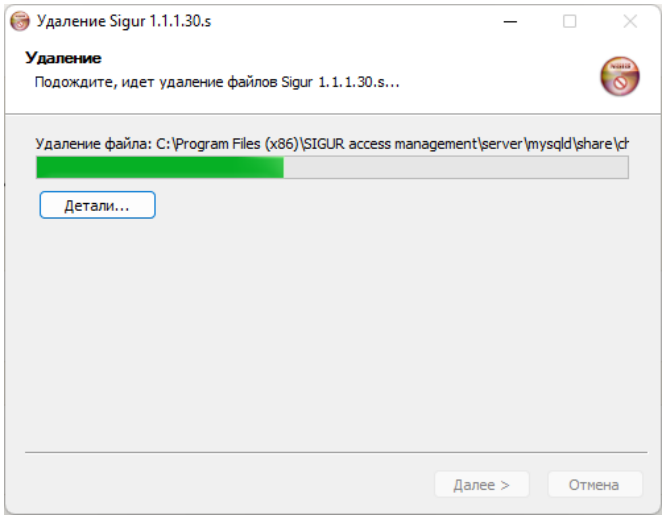


Запрос сохранения базы данных.

При нажатии кнопки «Да» в каталоге установки ПО будет создан файл с расширением .sql - копия базы данных на этот момент времени. Имя файла будет содержать текущую дату, например «2022-11-21.sql».

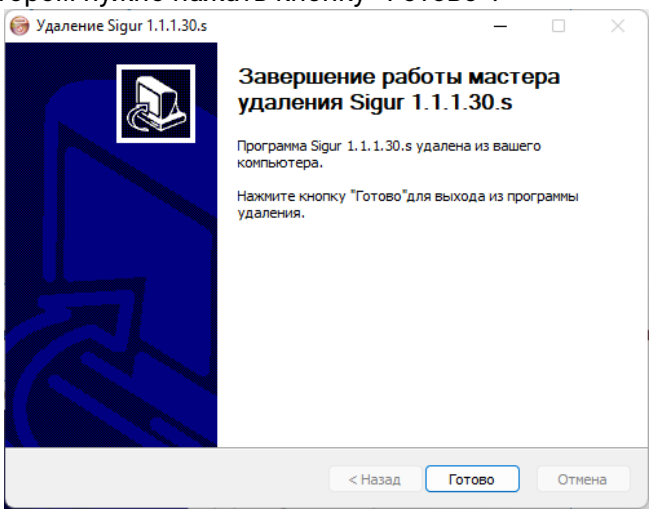
Обратите внимание, лицензия ПО Sigur при создании бэкапа базы не сохраняется, её необходимо предварительно сохранять отдельно!

По завершению создания бэкапа базы (или при отказе от него) будет открыто окно «Удаление», в котором будет отображаться процесс удаления программы.



Процесс удаления программы.

После завершения процесса откроется окно «Завершение работы мастера удаления», в котором нужно нажать кнопку «Готово».



Завершение работы мастера удаления.

Последним откроется окно с сообщением об удачном удалении программы, где нужно нажать «ОК». Удаление программы успешно завершено.

ОС Linux

- Debian
  Пример команды для удаления ранее установленных пакетов:

  sudo dpkg -r spnxclient spnxserver

- ОС Red Hat Linux
  Пример команды для удаления ранее установленных пакетов:

  $ sudo rpm -e spnxclient spnxclient-libs spnxserver

Данные команды никак не затрагивают саму БД, т.к. в случае сервера под управлением Linux она администрируется штатными средствами mysql.

7.4. Обновление системы «Sigur»

ОС Windows

Перед обновлением с версии ПО 1.2.x.x до версии 1.6.0.1 рекомендуется обратиться в техническую поддержку Sigur.

Для обновления сервера необходимо закрыть все графические окна программы и запустить файл setup-XX.exe (где XX – номер версии ПО), аналогичный тому, из которого производилась установка системы. Установщик определит необходимость и возможность обновления автоматически.

По окончании обновления запустите программу управления сервером и нажмите кнопку «Старт» на вкладке «Состояние».

Если при этом потребуется обновление версии базы данных - программа выдаст соответствующий запрос, в ответ на который следует согласиться, нажав кнопку «Да». Никакие данные при этом не будут потеряны.

Клиентские места системы, установленные под Windows, достаточно перезапустить, после чего они обновятся автоматически.

Если в операционной системе настроены политики безопасности, то для автообновления клиентских мест обязателен доступ программы к:

- каталогу установки программы;
- ветке реестра HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\ACS Sphinx (для

32-битных версий Windows);
- ветке реестра HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\ACS Sphinx (для 64-битных версий Windows).

Дополнительно, при использовании интеграции с системой Ewclid, предоставить доступ к:

- ветке реестра HKLM\SOFTWARE\ComCom\Ewclid-AV\EventSystem\External;
- ветке реестра HKLM\SOFTWARE\ComCom\Ewclid-AV\EventSystem\Transport.

Клиентские места, установленные под ОС Linux, необходимо обновить вручную.

ОС Linux

Обновление выполняется поверх ранее установленных пакетов.

Пример готовой команды для **Linux Debian**:

$ sudo dpkg -i spnxclient_*all.deb spnxserver_*.deb

Пример готовой команды для **Red Hat Linux**:

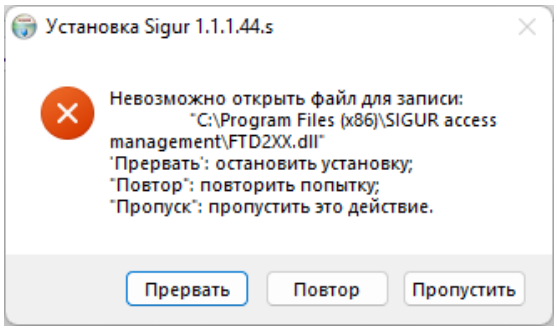
$ sudo rpm -U spnxclient-y.y.y.y-0.noarch.el7.rpm spnxclient-libs-y.y.y.y-0.el7.x86_64.rpm spnxserver-y.y.y.y-0.el7.x86_64.rpm

где y.y.y.y - новая версия пакета, например "1.1.1.40".

В случае ОС **Red Hat Linux** все обновляемые пакеты обязательно должны быть перечислены сразу, а не поодиночке.

7.4.1. Возможные сообщения об ошибках при обновлении ПО

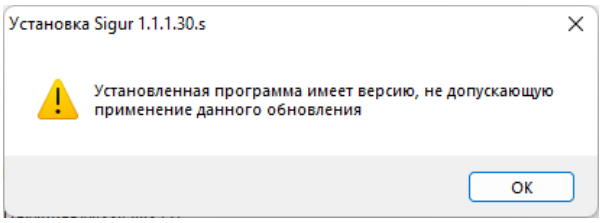
- После запуска установочного файла появляется сообщение «Невозможно открыть файл для записи: "C:\Program Files (x86)\SIGUR access managment\FTD2XX.dll"»:



Пример возможной ошибки в процессе установки.

Данная ошибка возникает в том случае, если перед запуском файла установщика не были закрыты все графические окна программы («Управление сервером», «Клиент»), в т.ч. запущенные в сеансах других пользователей ПК.

- При попытке запустить обновление ПО открывается окно «Установленная программа имеет версию, не допускающую применение данного обновления»:



Пример ошибки при запуске мастера установки.

Данное сообщение возникает в случае запуска файла-установщика той же либо более ранней версии ПО «Sigur», чем уже установленная на данном ПК.

7.5. Перенос сервера на другой компьютер (Windows)

Для перемещения сервера системы на другой компьютер нужно выполнить следующие действия:

1. В случае использования программной или комбинированной лицензии в программе «Клиент» в меню «Файл - Управление модулями» выберите «Сохранить лицензию в файл», указав каталог сохранения файла лицензии.
2. Запустите программу «Управление сервером».
3. Сохраните базу данных (БД). Для этого нажмите «Экспорт базы» на закладке «База данных», введите имя файла и выберите путь, отличный от папки установленной программы. При этом серверный модуль автоматически остановится, запускать его не нужно!

4. Установите ПО «Sigur» на новый компьютер.
5. Запустите на новом компьютере с помощью программы «Управление сервером» компонент «Сервер БД». На предложение о создании новой базы данных выберите «нет».
6. Произведите импорт БД. Для этого нажмите кнопку «Импорт базы» на закладке «База данных», выберите сохранённый ранее файл и нажмите кнопку «Открыть».
7. После завершения импорта текущая версия БД может не совпадать с нужной версией («старая» БД и «новое» ПО), в этом случае нажмите кнопку «Обновить».
8. Запустите компонент «Серверный модуль» на вкладке «Состояние».
9. Перенесите лицензию:

    - В случае хранения лицензии в памяти HASP-ключа, отключите его от старого сервера и подключите к новому компьютеру.
    - В случае использования программной лицензии загрузите ранее сохранённый файл лицензии (см.п.1) в программу «Клиент» через меню «Файл - Управление модулями», а далее обратитесь к «Руководству пользователя» или в техническую поддержку для привязки лицензии к новому компьютеру.
    - В случае использования программной лицензии, привязанной к HASP-ключу (комбинированной лицензии), необходимо подключить к новому серверу HASP-ключ и загрузить ранее сохранённый файл лицензии (см. п.1) в программу «Клиент» через меню «Файл - Управление модулями». Процесс переноса подробно описан в «Руководстве пользователя».
10. Укажите IP-адрес нового сервера СКУД в настройках каждого IP-контроллера. Инструкцию можно найти в разделе «Изменение IP-параметров устройства».

7.6. Переход с бесплатной версии ПО на платную

Для перехода с бесплатной версии системы на платную вставьте в сервер HASP-ключ аппаратной защиты или загрузите программную лицензию, а после - активируйте её и перезапустите ПО «Клиент».

8. Программа управления сервером

Программа управления сервером предназначена для наблюдения за состоянием компонентов сервера, настройки резервирования базы данных, редактирования настроек IP-контроллеров и так далее.

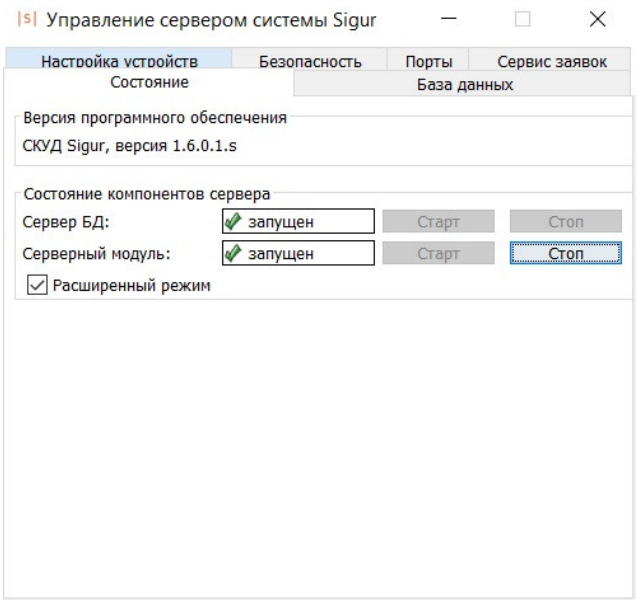
8.1. Запуск программы

Запуск программы осуществляется с помощью ярлыка «Управление сервером», расположенного в меню «Пуск» – «Программы» – «СКУД Sigur».

8.2. Главное окно программы

Главное окно программы предоставляет пользователю все средства для управления сервером системы «Sigur» и наблюдения за состоянием его компонентов.

Внешний вид главного окна программы:



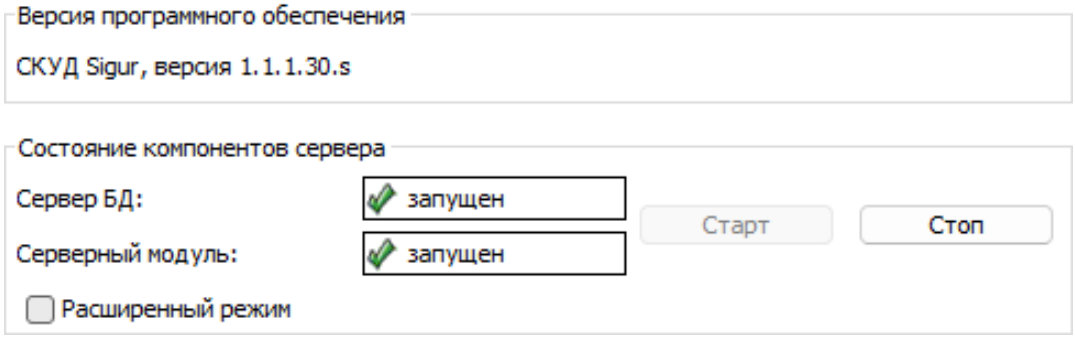
Окно программы управления сервером, вкладка «Состояние».

Программное обеспечение сервера состоит из двух программных компонентов. Сервер базы данных предоставляет доступ всем программным компонентам системы к общей базе данных. Серверный модуль обеспечивает информационный обмен с контроллерами системы по линиям связи, а также информационный обмен сервера с клиентскими местами. Для нормальной работы системы оба компонента должны быть запущены.

Функции управления сервером СКУД распределены по вкладкам: «Состояние», «База данных», «Настройка устройств», «Безопасность», «Порты», «Сервис заявок».

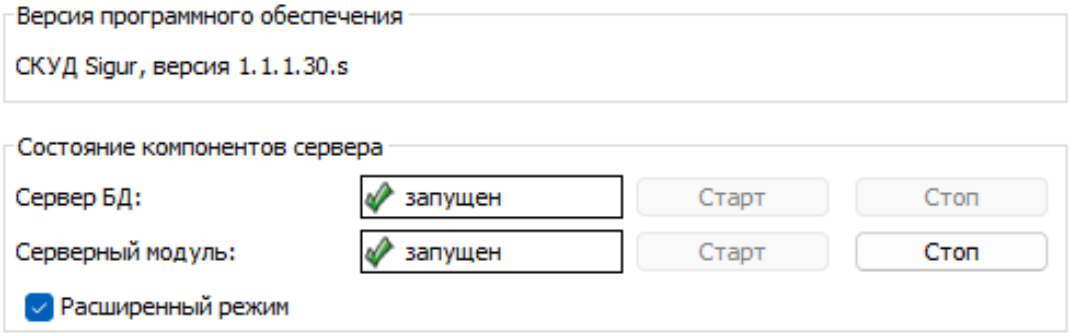
9. Управление компонентами сервера

На вкладке «Состояние» можно запускать, останавливать компоненты сервера и наблюдать за их состоянием.
В верхнем окне вкладки отображается текущая версия программного обеспечения.
Обычный режим управления компонентами сервера:



Обычный режим управления компонентами сервера.

Расширенный режим управления компонентами сервера:



Расширенный режим управления компонентами сервера.

Для переключения режима управления служит функция «Расширенный режим». При выключенном расширенном режиме можно запускать и останавливать сразу оба компонента, при включённом – раздельно.

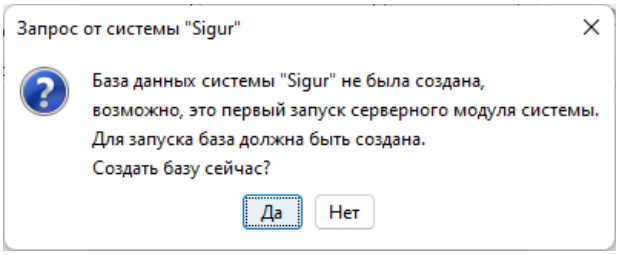
Запуск компонентов осуществляется кнопкой «Старт» в строке нужного компонента. Остановка компонентов осуществляется кнопкой «Стоп» в строке нужного компонента.

Состояние компонента отображается в виде «Запускается», «Запущен», «Останавливается», «Остановлен» или «Не готов».

9.1. Управление сервером БД

Запуск сервера БД осуществляется кнопкой «Старт» в строке «Сервер БД».

При первом запуске сервера БД после установки программного обеспечения откроется окно с запросом о создании новой базы данных.



Окно с запросом создания базы данных.

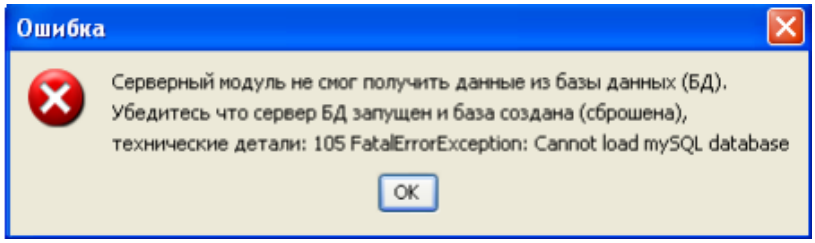
Нажав кнопку «Да», создаём исходную базу данных. База создаётся один раз, и последующие запуски происходят без этого запроса.

Нажав кнопку «Нет», можно отказаться от создания базы данных, при этом сервер БД будет запущен, но работа остальных компонентов ПО при этом невозможна. Для создания БД можно также нажать кнопку «Сбросить базу» во вкладке «База данных».

Остановка сервера БД осуществляется кнопкой «Стоп» в строке «Сервер БД».

9.2. Управление серверным модулем

Запуск серверного модуля осуществляется кнопкой «Старт» в строке «Серверный модуль». Запуск серверного модуля при остановленном сервере БД автоматически запустит и серверный модуль, и сервер БД.
При запуске серверного модуля с повреждённой базой данных программа выдаст следующее сообщение об ошибке.

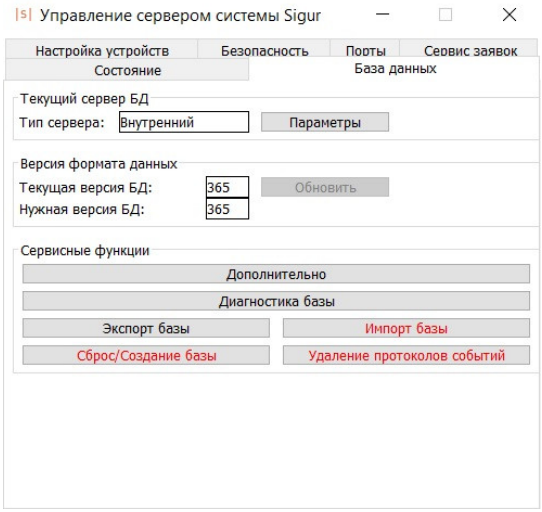


Сообщение при запуске серверного модуля с повреждённой базой данных.

Для устранения повреждений см. раздел «Диагностика (ремонт) базы данных».

10. Управление базой данных

Вкладка «База данных» предназначена для всех операций, возможных с базой данных СКУД «Sigur».



Окно программы управления сервером, активна вкладка «База данных».

База данных используется системой для хранения информации об объектах доступа, режимах допуска, о событиях системы и т.д.

По умолчанию системой используется БД MariaDB.

10.1. Версия формата данных

Отображаются номера текущей и необходимой версий базы данных. Для нормальной работы системы они должны совпадать.

Панель «Версия формата данных».

Версия БД – это характеристика базы данных, используемой программой. По мере усовершенствования системы, введения в неё новых функций и выхода новых версий ПО, может меняться формат хранения данных и, соответственно, меняется версия БД.

В ячейке «Текущая версия БД» отображается версия базы данных системы в текущий момент. В ячейке «Нужная версия БД» отображается версия, необходимая для работы системы. Обычно эти значения совпадают, при несовпадении необходимо выполнить обновление версии БД.

10.2. Обновление версии базы данных

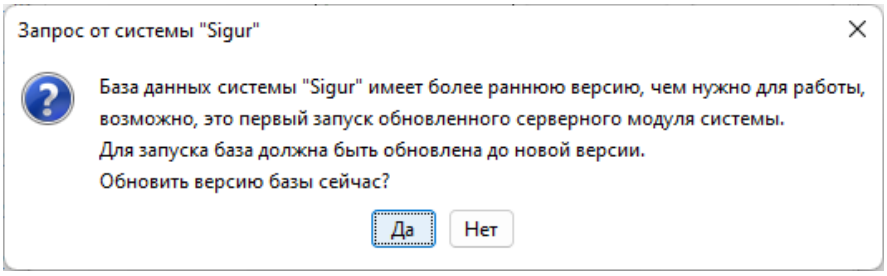
После обновления программного обеспечения или после импорта старой версии БД возможна ситуация, когда значение в ячейке «Нужная версия БД» станет больше, чем значение «Текущая версия БД». При этом активируется кнопка «Обновить».

Пример отличия версий БД.

Для обновления текущей версии БД нужно нажать кнопку «Обновить».

Программа откроет окно «Обновляем версию базы», в котором будет отображаться процесс обновления. После успешного завершения процесса окно закроется.

Если обновление программного обеспечения или импорт старой версии базы данных были сделаны при остановленном сервере БД, то при первом же запуске сервера программа выдаст запрос на обновление версии базы данных.

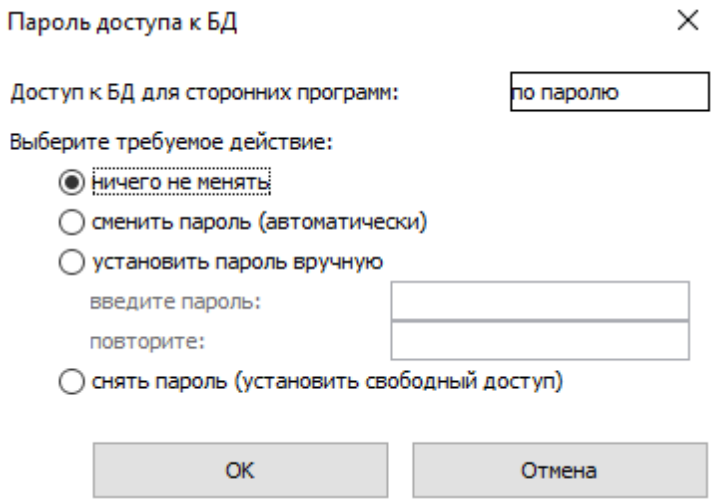


Сообщение при запуске сервера БД после обновления серверного ПО.

Нажмите кнопку «Да», после чего версия БД будет обновлена до необходимой.

10.3. Установка пароля на доступ к базе данных для сторонних программ.

Для изменения доступа к БД необходимо на вкладке «База данных» нажать кнопку «Параметры», далее – кнопку «Изменить».



Окно «Пароль доступа к БД».

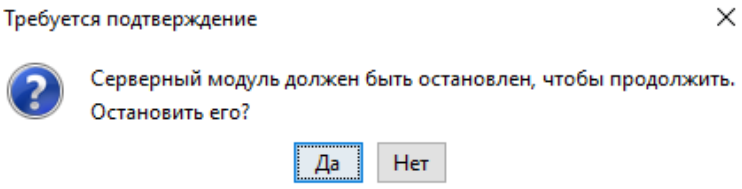
После чего в появившемся окне «Пароль доступа к БД» можно выбрать следующие функции:

- «ничего не менять».

При выборе данного пункта после нажатия кнопки «OK» доступ останется прежним.

- «сменить пароль (автоматически)».

После нажатия кнопки «OK» пароль будет сформирован программой автоматически случайным образом. При этом фактически исключается доступ сторонних программ к БД. В процессе изменения пароля появится окно с запросом на остановку серверного модуля. Для продолжения нажмите «Да», затем запустите серверный модуль на вкладке «Состояние».



Окно подтверждения остановки серверного модуля.

- «установить пароль вручную».

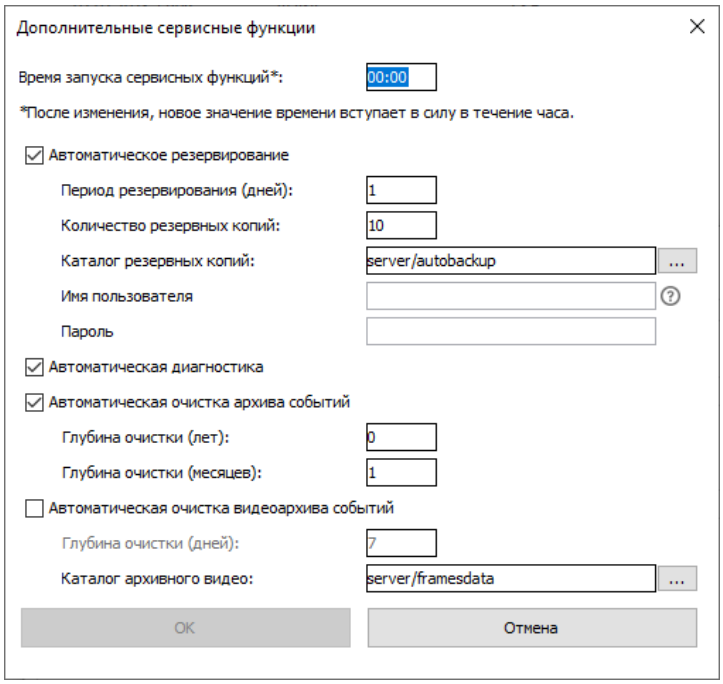
Позволяет самостоятельно задать пароль для БД. После ввода пароля, его подтверждения и нажатия кнопки «OK» появится окно с запросом на остановку серверного модуля. Нажмите «Да», затем запустите серверный модуль на вкладке «Состояние».

- «снять пароль (установить свободный доступ)».

Убирает пароль с БД. После нажатия кнопки «OK» появится окно с запросом на остановку серверного модуля. Нажмите «Да», затем запустите серверный модуль на вкладке «Состояние».

10.4. Дополнительные настройки сервера

Для настройки дополнительных функций сервера на вкладке «База данных» нажмите кнопку «Дополнительно».



Дополнительные функции сервера.

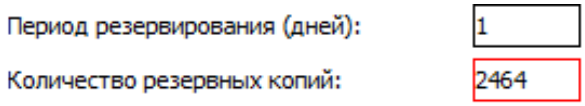
10.5. Автоматическое резервирование (сохранение) базы данных

Для включения автоматического сохранения БД необходимо:

1. На вкладке «База данных» нажать кнопку «Дополнительно».
2. Включить опцию «Автоматическое резервирование».
3. Ввести нужный период резервирования (от 1 до 999), определяющий, через сколько дней программа будет сохранять очередную резервную копию БД. В нужный день периода процедура резервирования базы начнётся в указанное «Время запуска сервисных функций» (по умолчанию - это 0 часов 0 минут).
4. Ввести количество последних резервных копий (от 1 до 999), которое будет хранить программа.
5. Изменить, при необходимости, каталог для сохранения резервных копий. Рекомендуется сделать это сразу же, чтобы хранить копии на другом физическом носителе или хотя бы на другом логическом диске.

При неверном вводе, рамка вокруг поля ввода значения меняет цвет на красный.

Пример окна, где первое значение введено корректно, а второе - нет:



Пример ввода некорректного значения.

По умолчанию резервные копии БД сохраняются программой в каталог установленной программы: «...\SIGUR access management\server\autobackup\», где «...» – путь установки программы (обычно «C:\Program files (x86)\»).

Формат сохраняемых файлов: ГГГГ–ММ–ДД.sql. Название файла определяет год, месяц и день автосохранения.

Старые копии автоматически удаляются.

10.6. Автоматическая диагностика базы данных

Для работы данной функции на вкладке «База данных» нажмите кнопку «Дополнительно» и включите опцию «Автоматическая диагностика». При этом программа проводит автоматическую проверку базы раз в сутки, начиная эту процедуру в указанное «Время запуска сервисных функций» (по умолчанию - это 0 часов 0 минут).

10.7. Автоматическая очистка архива событий

Для работы данной функции на вкладке «База данных» нажмите кнопку «Дополнительно» и включите опцию «Автоматическая очистка архива событий» и введите нужную глубину очистки архива: лет + месяцев. Все события архива старше указанного срока будут удаляться.

10.8. Автоматическая очистка видеоархива событий

Для работы данной функции на вкладке «База данных» нажмите кнопку «Дополнительно» и включите опцию «Автоматическая очистка видеоархива событий» и введите нужную глубину очистки видеоархива в днях. Все события видеоархива старше указанного срока будут удаляться.

По умолчанию видеоархив сохраняется программой в каталог установленной программы: «...\SIGUR access management\server\framesdata\», где «...» – путь установки программы (обычно «C:\Program files (x86)\»).

10.9. Сохранение (экспорт) базы данных

Ручное сохранение БД можно использовать для создания резервных копий, которые в дальнейшем можно использовать для восстановления системы после серьёзного сбоя, вызвавшего повреждение структуры БД, или для переноса сервера системы на другой компьютер.

Для сохранения резервной копии на компьютере-сервере под управлением ОС Windows необходимо на вкладке «База данных» нажать кнопку «Экспорт базы». Программа предложит выбрать путь и ввести имя сохраняемого файла. Полученный файл можно сохранить на любом носителе и использовать в дальнейшем для восстановления системы или переноса системы на другой сервер.

Для дальнейшей работы системы необходимо запустить серверный модуль на вкладке «Состояние».

В случае компьютера-сервера под управлением ОС Linux администрирование БД осуществляется с помощью штатных средств mysql.

В частности, для создания бекапа можно использовать следующую команду:

mysqldump -u <user> -P 3306 -p <userpass> -B TC-DB-MAIN TC-DB-LOG > backup.sql

где:

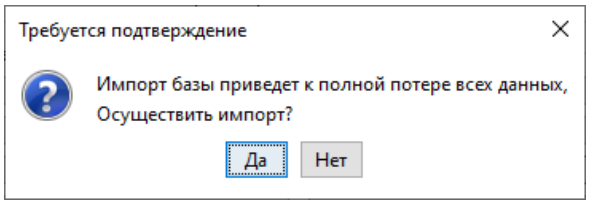
- <user> - имя пользователя БД;
- <userpass> - пароль указанного пользователя БД;
- TC-DB-MAIN, TC-DB-LOG - наименования используемых БД.

10.10. Восстановление (импорт) базы данных

Операция импорта базы данных является потенциально опасной, так как приводит к полной потере всех данных, содержащихся в текущей БД.

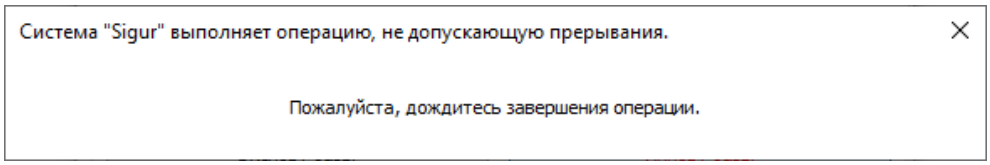
Импорт базы данных может потребоваться при переносе системы на другой компьютер или серьёзном сбое, вызвавшем повреждение структуры БД, которое неустранимо с помощью операции «Диагностика базы данных».

В случае сервера под управлением ОС Windows для импорта БД из резервной копии необходимо на вкладке «База данных» нажать кнопку «Импорт базы». Программа запросит подтверждение операции.



Запрос подтверждения импорта БД.

При нажатии кнопки «Да» программа предложит выбрать файл с сохранённой базой данных. После выбора файла и нажатия кнопки «Открыть» появится информационное окно, которое автоматически закроется при завершении импорта.



Информационное окно при импорте базы данных.

После завершения импорта необходимо проверить соответствие текущей версии БД и нужной версии БД. Если текущая версия БД меньше нужной, необходимо обновить ее, нажав кнопку «Обновить» на панели «Версия формата данных».

В случае сервера под управлением ОС Linux администрирование БД осуществляется с помощью штатных средств mysql. В частности, для загрузки готового бекапа в систему можно воспользоваться следующей командой:

mysql -u <user> -P 3306 -p <userpass> < backup.sql

где:

- <user> - имя пользователя БД;
- <userpass> - пароль указанного пользователя БД;
- *backup.sql* - наименование импортируемого файла с бекапом БД.

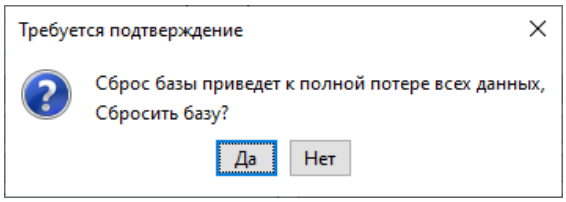
Обратите внимание, если файл бекапа первоначально был сформирован на сервере под управлением ОС Windows, в настройках сервера БД необходимо отключить чувствительность к регистру (см. раздел «Установка системы Sigur»).

10.11. Сброс/создание базы данных

Операция сброса базы данных является потенциально опасной, так как приводит к полной потере всех данных, содержащихся в текущей БД.

Выполнение данной операции требуется только в случае необходимости создания чистой базы данных.

Для сброса БД нужно нажать кнопку «Сброс/создание базы». Программа запросит подтверждение потенциально опасной операции.

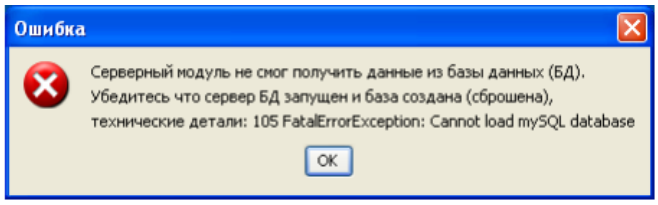


Запрос подтверждения сброса базы данных.

10.12. Диагностика (ремонт) базы данных

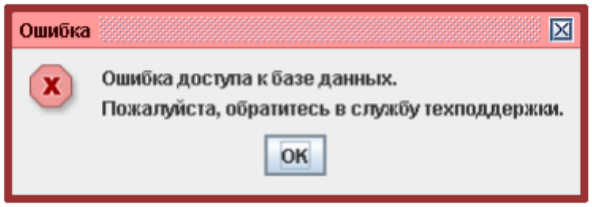
Эта функция позволяет устранять некоторые повреждения данных, возникшие, например, в результате аварийного завершения работы системы (зависание, выключение питания компьютера и т.д.).

Следствием таких повреждений является невозможность работы системы. Серверный модуль при этом может выдавать ошибку получения данных.



Ошибка серверного модуля.

При работе клиентского ПО может возникать ошибка доступа к базе данных.



Ошибка доступа к базе данных.

Для исправления повреждений необходимо запустить диагностику, нажав на вкладке «База данных» кнопку «Диагностика базы».

После нажатия откроется окно «Диагностируем базу данных», в котором отображается прогресс операции и комментарии к нему. При успешном окончании процесса это окно автоматически закроется, в случае обнаружения/исправления каких-то серьёзных ошибок окно останется открытым и заполненным сообщениями об обнаруженных проблемах.

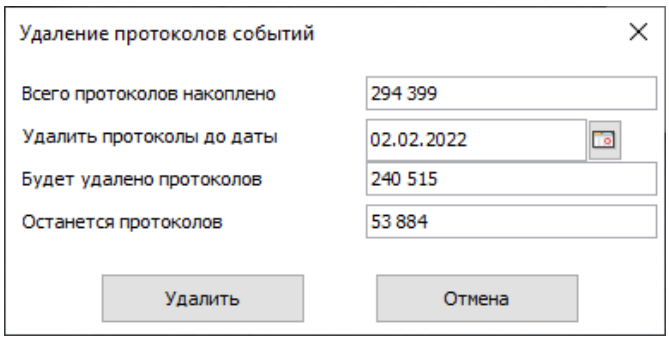
Если после этого сообщения об ошибках продолжают появляться – обратитесь в службу технической поддержки.

10.13. Удаление протоколов событий

Эта функция позволяет удалять протоколы до определённой даты. Для удаления на вкладке «База данных» нажмите кнопку «Удалить протоколы событий».

В появившемся окне удаления протоколов доступны следующие данные:

- «Всего протоколов накоплено» - отображает полное количество протоколов в базе данных.
- «Удалить протоколы до даты» - позволяет выбрать дату, до которой включительно будут удалены протоколы.
- «Будет удалено протоколов» - отображает количество протоколов, которые будут удалены.
- «Останется протоколов» - отображает количество протоколов, которое останется после удаления.

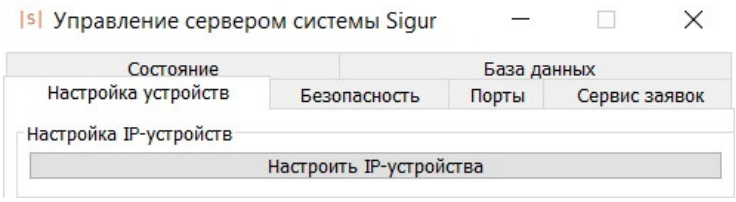


Окно удаления протоколов событий.

Выберите дату, до которой включительно надо удалить протоколы, и нажмите «Удалить», затем подтвердите операцию.

11. Настройка IP–устройств

На вкладке «Настройка устройств» можно производить настройку IP-параметров контроллеров «Sigur», а также просматривать список доступных на текущий момент в сети устройств.



Вкладка «Настройка устройств».

11.1. Добавление и настройка IP–устройств

Контроллеры Sigur нового поколения (E510, E2, E4) сразу отображаются в списке при первом запуске и не требуют добавления вручную. Контроллеры предыдущих поколений не имеют IP-адреса по умолчанию, при первом подключении необходимо задать им IP-параметры вручную, воспользовавшись кнопкой «Добавить новое устройство».

Предполагается, что ваш компьютер настроен на работу в компьютерной сети по протоколу IPv4 (это справедливо для большинства офисных компьютеров) и сетевой интерфейс, через который будет организована связь с контроллером, имеет статический IP-адрес. Если вы не уверены в этом - обратитесь к системному администратору, либо в нашу техподдержку.

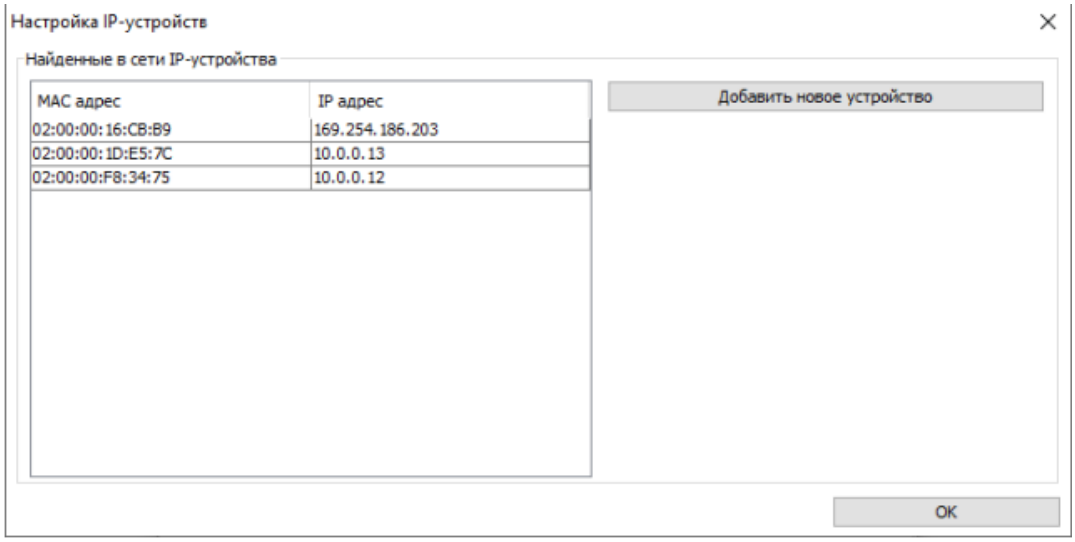
Предварительно отключите на всякий случай сетевые фильтры («файрволы») и программы антивирусной защиты. После проведения настройки включите их и убедитесь, что СКУД функционирует нормально. Если при этом контроллер пропадёт из списка найденных устройств или с ним пропадёт связь в программе «Клиент» (на вкладке «Оборудование») - значит требуется настроить файрвол/антивирус: разрешить работу программных модулей «Sigur», доступ к определённым портам и т.п.

Для добавления нового IP-устройства СКУД «Sigur» или изменения IP-параметров уже добавленного устройства запустите программу «Управление сервером»: Пуск → Все программы → СКУД Sigur → Управление сервером. Выберите вкладку «Настройка IP-устройств» и нажмите кнопку «Настроить IP-устройства».

Запуск программы управления сервером возможен как на сервере СКУД, так и на любом другом компьютере (например, если новый контроллер расположен в

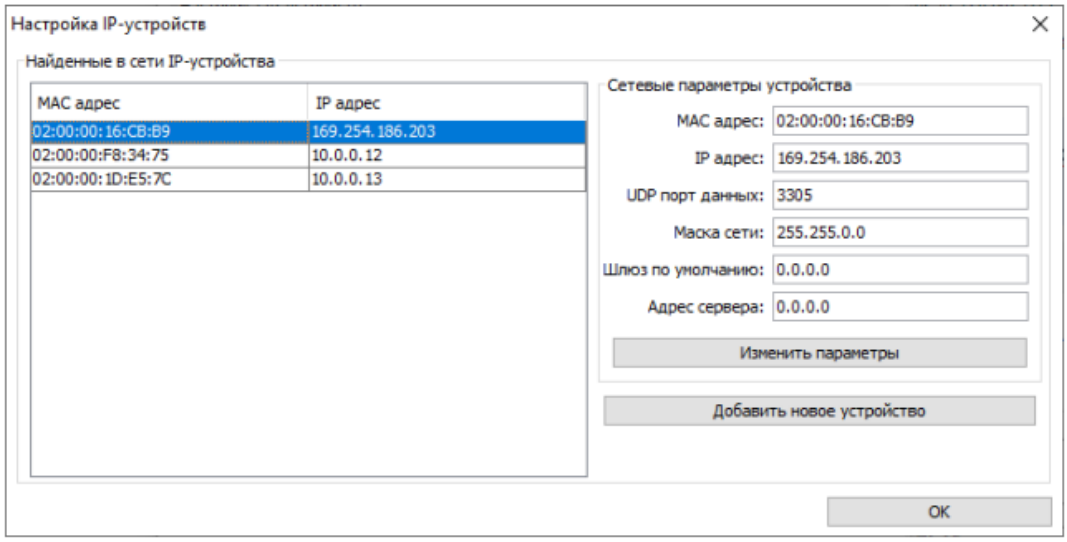
другой подсети, до которой не дойдут широковещательные запросы). При этом не требуется запуск компонентов сервера (сервер БД и серверный модуль), вкладка «Настройка устройств» работает автономно, не требует наличия лицензий.

Открывшееся окно содержит список устройств с уже настроенными IP-параметрами (и до которых доходят широковещательные запросы в этом сегменте IP-сети), а также кнопки «Добавить новое устройство».



Список найденных в сети IP-устройств.

При выборе в списке конкретного устройства в правой области окна для него отображаются текущие IP-параметры и доступна кнопка «Изменить параметры».



Параметры выбранного устройства в списке найденных в сети IP-устройств.

Далее возможны два варианта.

1. В списке «Найденные в сети IP-устройства» уже присутствует строка с MAC адресом вашего контроллера. В таком случае выделите эту строчку и нажмите кнопку «Изменить параметры».
2. Список «Найденные в сети IP-устройства» пуст. В таком случае нажмите кнопку «Добавить новое устройство» и следуйте инструкциям, описанным далее.

11.1.1. Добавление нового устройства

Введите в соответствии с настройками вашей сети следующие параметры:

- MAC-адрес.

Введите значение MAC, напечатанное на наклейках, расположенных на крышке корпуса или на упаковке контроллера. Двоеточия-разделители можно опустить, иные разделители — не допускаются.

- IP-адрес.

Это адрес, который вы хотите присвоить контроллеру. Он должен относиться к диапазону адресов той сети, к которой подключён контроллер, и не быть занятым никаким другим сетевым оборудованием. В дальнейшем этот адрес будет использоваться для однозначной идентификации точки доступа СКУД (на вкладке «Оборудование» в программе «Клиент»).

- Маска сети.

Маска сети определяет, какая часть IP-адреса контроллера относится к адресу сети, а какая — к адресу самого контроллера в этой сети. Например, контроллер с IP-адресом 192.168.0.70 и маской подсети 255.255.255.0 находится в сети 192.168.0.X.
Заданная маска должна совпадать с маской сети, в которой будет работать контроллер. В самом простом случае, когда сервер и контроллер находятся в одной сети, посмотрите значение маски в свойствах сетевого подключения вашего компьютера.

- Шлюз.

Введите IP-адрес маршрутизатора, который обеспечивает выход в Интернет или другую сеть, в которой находится сервер «Sigur». Если контроллер и сервер находятся в пределах одной сети — значение в этом поле может быть произвольным.

- Адрес сервера, с которым будет работать контроллер.

Если вы настраиваете контроллер с компьютера — сервера СКУД, то выберите опцию «На этом компьютере, используя интерфейс», и далее в выпадающем списке выберите IP-адрес нужного сетевого интерфейса.
Если вы осуществляете настройку, например, с ноутбука, а контроллер в дальнейшем будет работать с другим сервером - выберите опцию «На другом

компьютере, имеющем IP адрес», и введите адрес настоящего сервера.

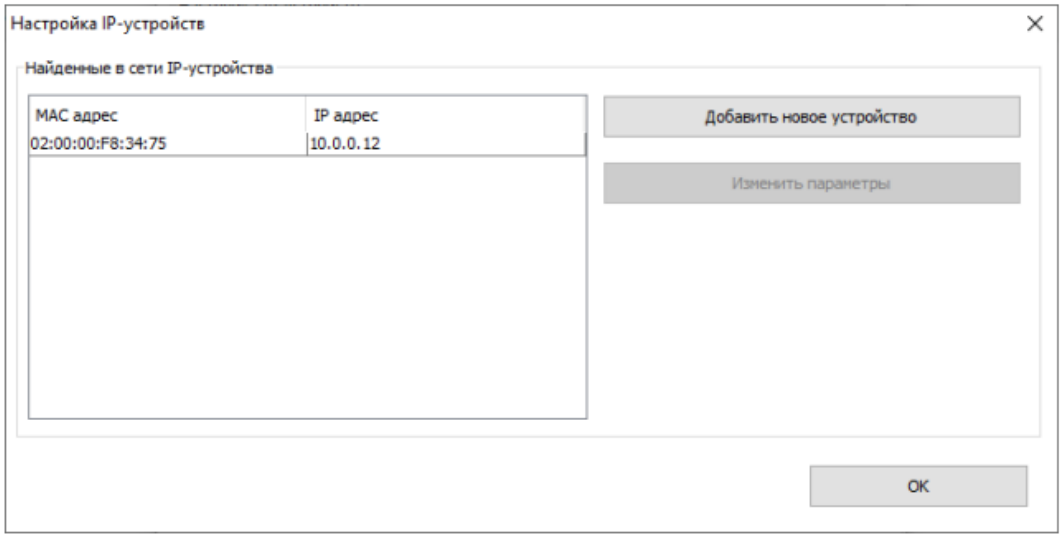
- Пароль.

Значение пароля по умолчанию уже введено в поле.

При необходимости изменения пароля следует выделить пункт «Изменить пароль», после чего станут доступны поля для ввода и подтверждения нового пароля.

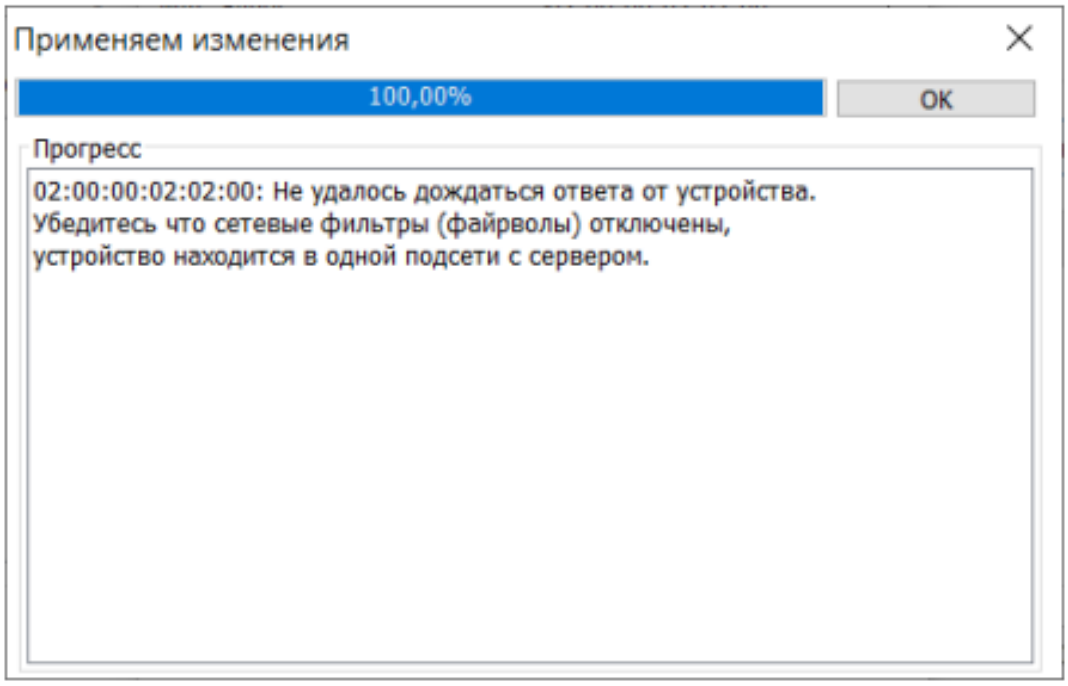
Явные ошибки вводимых данных отображаются красным цветом рамки панели ввода. При этом становится неактивной кнопка «ОК», не давая применять заведомо некорректные настройки. После ввода всех настроек нажмите «ОК».

При успешном завершении процесса в списке устройств появится строка с MAC и IP-адресами настроенного контроллера.



Успешно настроенный контроллер.

Если же программа выдаст сообщение об ошибке - значит по какой-либо причине серверу не удалось «достучаться» до контроллера.

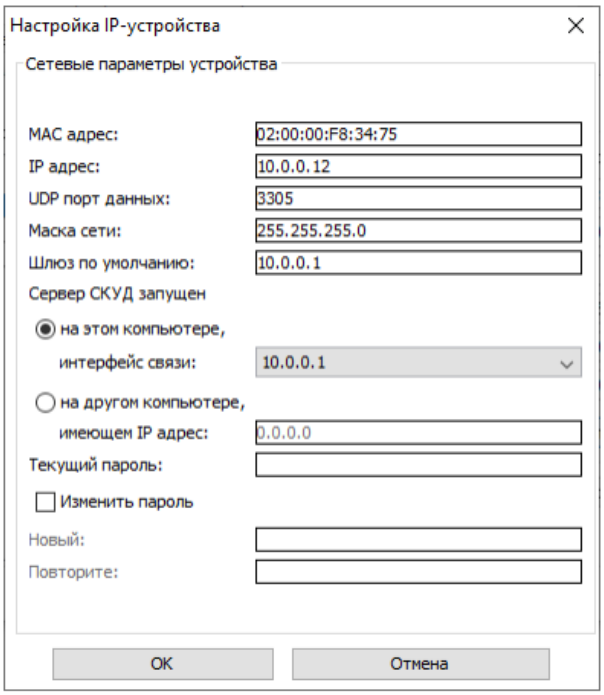


Ошибка при попытке настройки IP-параметров.

11.1.2. Изменение IP-параметров устройства

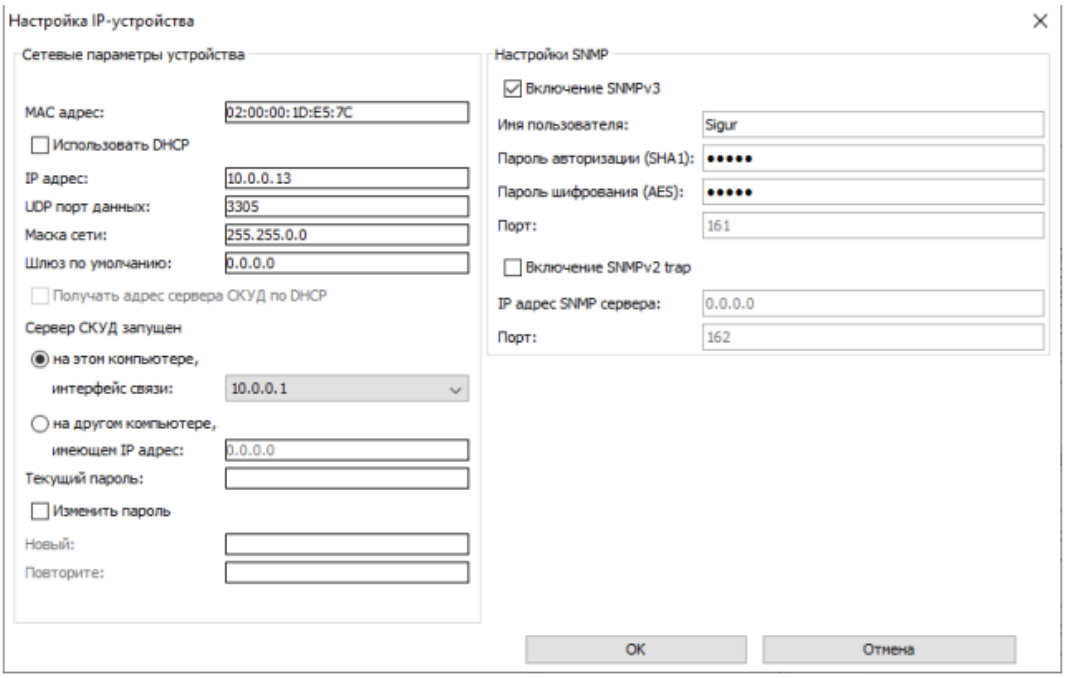
Для изменения IP-параметров выберите в списке нужный контроллер и нажмите кнопку «Изменить параметры». В зависимости от модели контроллера (и, соответственно, поддерживаемых им функций) открывающееся окно «Настройка IP-устройства» имеет разный вид.

- Для моделей E500U, R900U, E300, E300H, E100, E500, E900I, а так же преобразователей Sigur Orion и Sigur Rubezh имеет вид, представленный на рисунке «Настройка IP–устройств, вариант 1».



Окно «Настройка IP-устройства», вариант 1.

- Для моделей E510, E2, E4, E310 имеет вид, представленный на рисунке «Настройка IP–устройств, вариант 2», и представляет собой расширенный вариант окна редактирования параметров. Область «Сетевые параметры устройства» предназначена для настройки IP-параметров контроллера.



Окно «Настройка IP-устройства» вариант 2.

Перед завершением настроек в поле «Текущий пароль» введите пароль (значение по умолчанию см. в документе на соответствующую модель).

Для всех найденных в сети устройств возможно групповое изменение некоторых IP параметров. При выделении необходимой группы нажатие кнопки «Изменить параметры» позволит переопределить маску сети, шлюз по умолчанию, IP-адрес сервера СКУД и изменить пароль.

Получение IP-параметров по DHCP

Поддерживается не всеми моделями контроллеров. Наличие поддержки данной функции проверяйте в разделе «Технические характеристики» руководства по эксплуатации на конкретную модель контроллера.

Контроллеры можно настроить как на работу со статическим IP-адресом, назначенным вручную, так и на динамическое получение IP-параметров от DHCP-сервера. Режим работы определяется опцией «Использовать DHCP». При установленной галочке «Использовать DHCP» поля для ввода IP-адреса, UDP-порта, маски сети и шлюза не активны. При необходимости можно так же активировать получение адреса сервера от DHCP-сервера (для корректной работы функции требуется провести дополнительные настройки на стороне DHCP-сервера).

Передача статусов SNMP-серверу

Поддерживается не всеми моделями контроллеров. Наличие поддержки данной функции проверяйте в разделе «Технические характеристики» руководства по эксплуатации на конкретную модель контроллера.

В области «Настройки SNMP» можно включить функцию передачи статусов контроллера по протоколу SNMP.

11.1.3. Получение IP-параметров по DHCP

Функция получения IP-параметров по DHCP есть только у некоторых моделей контроллеров Sigur. Перед настройкой системы сверьтесь с техническими характеристиками контроллеров.

Контроллеры Sigur могут получать по DHCP следующий набор параметров:

- IP-адрес;
- маска сети;
- шлюз;
- адрес сервера Sigur.

На стороне контроллера должны быть включены опции «Использовать DHCP» и/или «Получать адрес сервера СКУД по DHCP». Контроллер поставляется с включённой опцией, а также она включается автоматически после сброса IP-параметров. Если ранее контроллеру были заданы статические IP-параметры, переключить его на работу по DHCP можно так же через ПО Sigur. Для этого:

1. Запустите программу «Управление сервером» в той же подсети, где работает контроллер.
2. Перейдите на вкладку «IP-устройства».
3. Выделите нужный контроллер в списке и нажмите кнопку «Изменить параметры».
4. Включите опции «Использовать DHCP» и, если необходимо, «Получать адрес сервера СКУД по DHCP». Поля для ручного ввода IP-параметров при этом станут неактивны.
5. Введите пароль доступа к настройкам контроллера (по умолчанию - «sigur») и нажмите «ОК».

Для назначения IP-адреса устройств, передачи им значений маски подсети и шлюза на стороне DHCP-сервера в общем случае не требуются дополнительные настройки. Если же требуется передавать контроллерам Sigur также адрес сервера СКУД, необходимо обеспечить следующее: при получении DHCP-сервером от устройства запроса на выдачу IP-адреса, если опция 60 соответствует значению «Sigur PACS Unit» (без кавычек), в ответе должно передаваться 4 байта IP-адреса сервера СКУД (в обратном порядке байт (актуально для 16 версии микропрограммы контроллера)) в опции 43, саб-опция 1.

Например, если необходимо сообщить контроллеру адрес сервера «172.19.40.10», то значение опции 43 должно быть следующим (в hex) - «01040A2813AC», где
01 - suboption;
04 - длина передаваемой полезной информации;
0A2813AC - IP-адрес сервера СКУД в обратном порядке байт. (hex) 0A 28 13 AC = (dec) 10 40 19 172

Используемые контроллером DHCP-опции.

Номер опции	Значение опции	Примечание
1	Маска подсети	Маска сети, в которой располагается контроллер.
3	Адрес основного шлюза	IP-адрес маршрутизатора, который обеспечивает выход в Интернет или другую сеть, в которой находится сервер «Sigur».
43	Специфичная информация производителя	Используется для указания IP-адреса сервера «Sigur». DHCP-сервер должен его вернуть в первой подопции (subpotion 1).
60	Идентификатор производителя	= Sigur PACS Unit

11.2. Возможные причины неудачной настройки IP-параметров

- Подключение контроллера к компьютеру (без использования промежуточного активного сетевого оборудования, например, коммутаторов) выполнено «прямым» кабелем.

Несмотря на то, что многие современные сетевые карты умеют автоматически определять тип подключения, рекомендуется использовать для таких соединений кроссоверный (он же «перекрёстный») кабель.
Несколько иллюстраций, помогающих понять способ обжима штекеров кабеля.

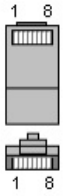


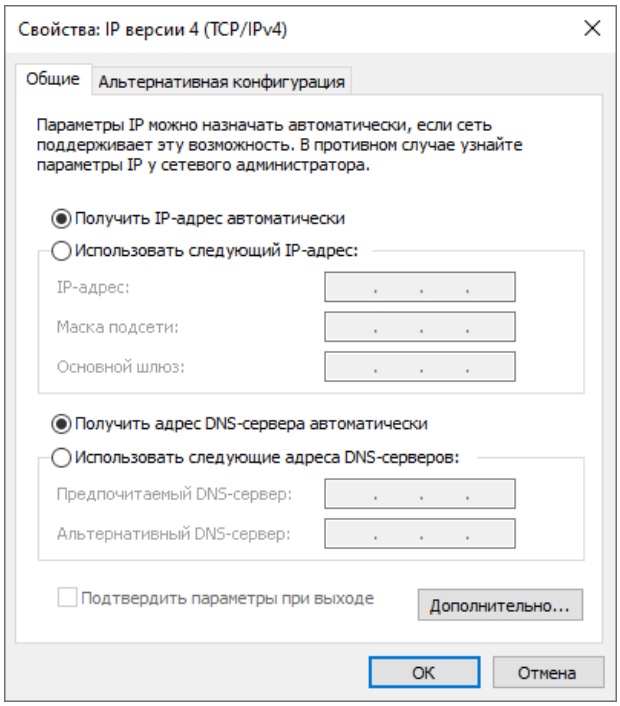
Рис. 39. Нумерация контактов разъёма RJ-45.

«Прямой» кабель для соединения с помощью коммутаторов.

«Перекрёстный» кабель для соединения «компьютер — контроллер».

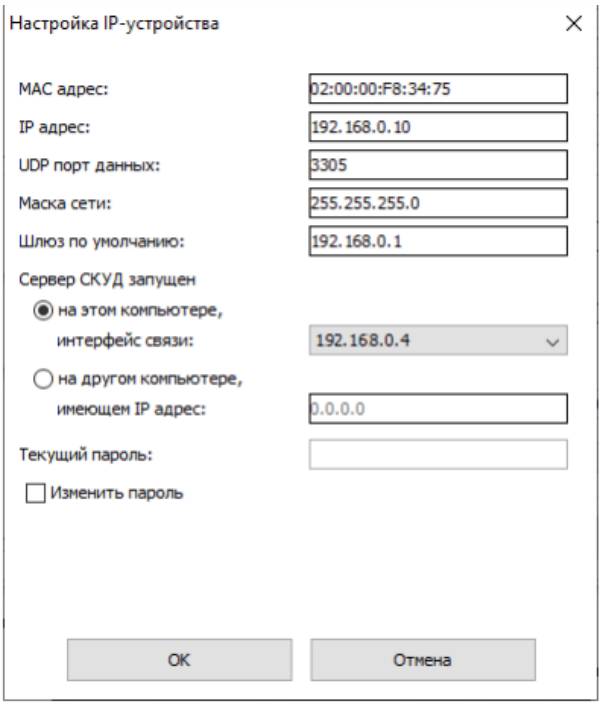
- Некорректные настройки сетевых интерфейсов Windows.

Например, два сетевых интерфейса компьютера настроены на работу в одной и той же IP-сети (имеют IP-адреса из одного диапазона и одинаковые маски), или на сервере включена динамическая IP-адресация (включена опция «Получить IP адрес автоматически»).

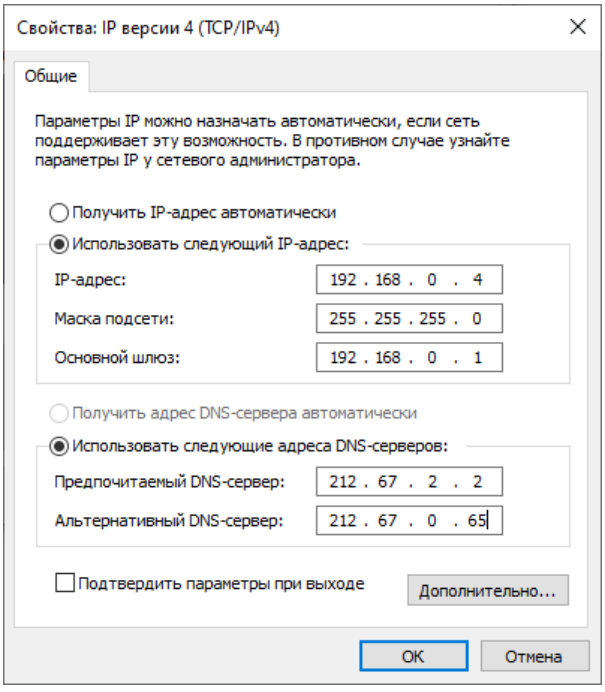


Неправильные настройки сетевого интерфейса для подключения контроллера.

Пример корректной настройки сервера и контроллера приведён ниже.



Пример правильной настройки контроллера.



Пример правильных настроек сетевого интерфейса сервера.

- Активность сетевых фильтров либо антивирусов.

Например, встроенный брандмауэр Windows иногда блокирует работу программы с сетевым интерфейсом без уведомления об этом пользователя. На

время настройки желательно отключить все программы, которые могут блокировать работу другого ПО или доступ к различным портам.

- Конфликт IP-адресов в сети.

При отсутствии связи с контроллером на вкладке «Оборудование» в программе «Клиент» (контроллер при этом виден в списке «Найденные в сети IP-устройства» программы «Управление сервером» и может успешно отвечать на команду ping) рекомендуется выключить питание контроллера и повторить команду ping. Сохранение отклика будет говорить о том, что в сети уже присутствует устройство с таким адресом и необходимо присвоить контроллеру другой свободный IP-адрес.

12. Возможные сообщения об ошибках при запуске серверного модуля

Сообщение об ошибке	Пояснение
Серверному модулю не удалось прочитать свой конфигурационный файл, технические детали: ...	Эти ошибки не должны появляться, если не изменять вручную файлы программы.
Серверный модуль отрапортовал некорректное значение конфигурационного параметра Com, технические детали: ...	
Серверный модуль не смог получить данные из базы данных (БД). Убедитесь что сервер БД запущен и база создана (сброшена), технические детали: ...	Выдаётся при попытке запуска серверного модуля при остановленном сервере БД.
Серверный модуль отрапортовал некорректную версию базы данных. Обновите версию БД. Технические детали: ...	Выдаётся при попытке запуска серверного модуля, когда текущая версия базы данных не соответствует требуемой. Обновите программное обеспечение либо базу данных (кнопка «Обновить» на вкладке «База данных»).
Серверный модуль системы «Sigur» не может быть запущен без ключа защиты. Вставьте ключ и повторите попытку запуска.	Эти ошибки могут появляться на более ранних версиях ПО при попытках запуска серверного стандартного (т.е. платного) ПО без ключа HASP.
Серверный модуль системы «Sigur» отказал в запуске из-за системы защиты. Убедитесь, что на компьютере не запущены никакие средства отладки и разработки. Не обращайте внимания на возможные сообщения об ошибках в приложении sphinxd.exe.	
Ошибка запуска серверного модуля системы «Sigur», вызванная защитой HASP, технические детали: ...	

13. Работа ПО Sigur с брандмауэрами (файрволами)

Запуск компонентов ПО Sigur на компьютере с работающим брандмауэром (файрволом) требует выполнения разрешающих настроек файрвола для ПО Sigur. В случае блокирования ПО Sigur его нормальная работа невозможна. Необходимые для работы ПО Sigur порты описаны в разделе «Порты, используемые системой по умолчанию».
Во многих случаях блокирование ПО «Sigur» происходит без каких-либо уведомлений для пользователя, что осложняет диагностику проблем.

14. Шифрование трафика между компонентами системы по TLS

Начиная с версии ПО 1.6.0.1, в Sigur реализовано шифрование трафика по протоколу TLS между частями системы для обеспечения безопасности передачи данных. Мы рекомендуем использовать встроенный функционал шифрования для исключения возможности перехвата и утечки конфиденциальной информации.

На текущий момент возможно зашифровать трафик по TLS между следующими компонентами системы:

1. Клиентские рабочие места Sigur - сервер Sigur.
2. Сторонние сервисы – веб-сервер Sigur (в рамках взаимодействия по REST API).
3. Сторонние сервисы – TCP-сервер Sigur (в рамках интеграционного протокола OIF).

По умолчанию используется незащищенное соединение. Выбор предпочтительного метода взаимодействия остается за пользователем системы. Функционал шифрования данных не лицензируется и доступен в бесплатной версии ПО.

На текущий момент ПО Sigur поддерживает протокол TLS версии 1.2 (Windows) и 1.3 (Linux).

14.1. Переход на небезопасное соединение и запрет подключения к серверу

Шифрование данных по TLS отключено в системе по умолчанию.

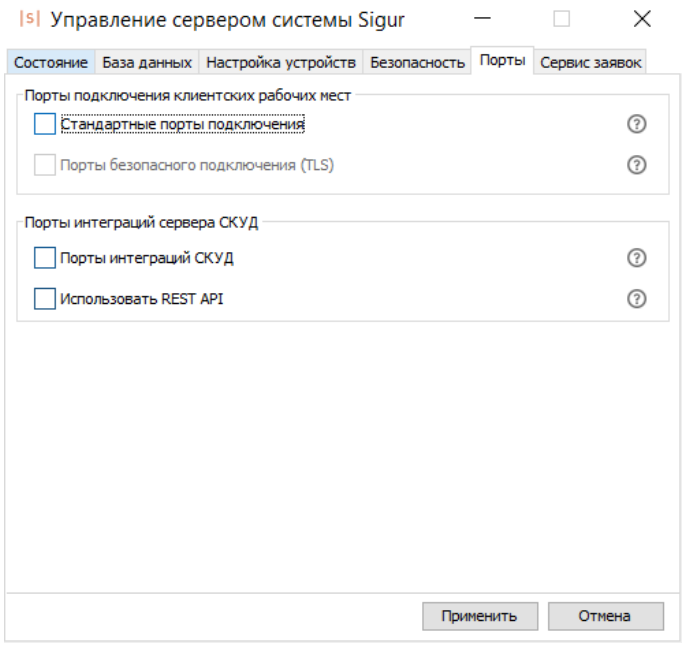
Пользователь может настроить параметры защищенного соединения, а также полностью или частично запретить подключение к сетевым портам сервера Sigur.

Рассмотрим доступные варианты конфигурации блока ПО «Управление сервером» - «Порты» - «Порты подключения клиентских рабочих мест»:

1. **Активен только чек-бокс «Порты безопасного подключения (TLS)».** Клиентские места Sigur могут использовать только зашифрованное соединение при подключении к серверу. Клиентская и серверная части должны быть сконфигурированы согласно инструкции в разделе «Установка зашифрованного соединения между клиентом и сервером Sigur».
2. **Активен только чек-бокс «Стандартные порты подключения».** Клиентские места Sigur могут использовать только незащищенное соединение при подключении к серверу. В диалоге ПО «Клиент» - «Выбор сервера» - «Параметры подключения» должен быть отключен чек-бокс «Использовать безопасное подключение».

3. **Активны оба чек-бокса.** Клиентские места Sigur могут использовать любой вид соединения, конфигурация каждого клиентского места настраивается отдельно.
4. **Выключены оба чек-бокса.** Клиентским рабочим местам Sigur запрещено подключаться к серверу Sigur.

В системе также есть возможность запретить подключение к порту REST API и к порту интеграционного протокола OIF, выключив соответствующие чек-боксы в блоке ПО «Управление сервером» - «Порты» - «Порты интеграций СКУД».



Запрет подключения к портам сервера Sigur.

Настройка безопасного соединения подробно описана в следующих разделах.

14.2. Установка зашифрованного соединения между клиентом и сервером

В данном разделе описан процесс настройки ПО Sigur для шифрования трафика между серверной и клиентской частями системы. Каждое клиентское рабочее место Sigur конфигурируется отдельно.

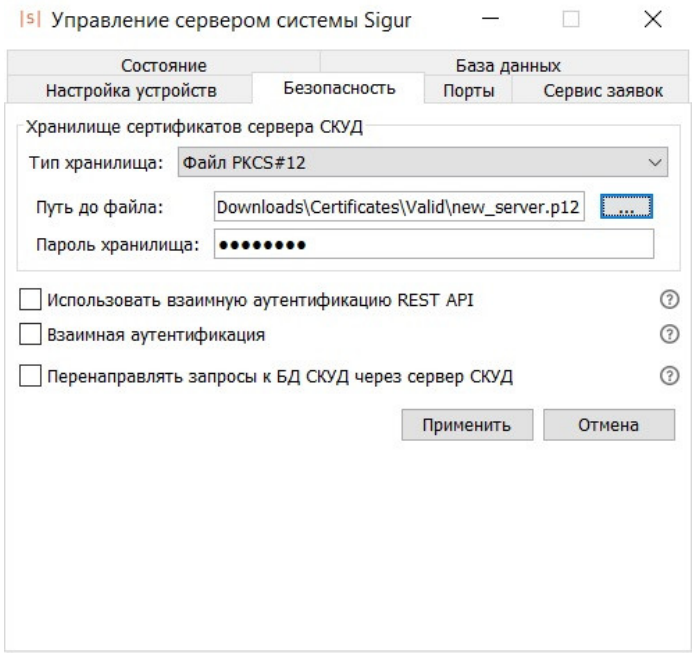
14.2.1. Настройка сервера Sigur

Для настройки серверной части СКУД необходимо:

1. Подготовить хранилище сертификатов безопасности сервера. Ознакомиться с требованиями к файлу хранилища Вы можете в данном разделе.

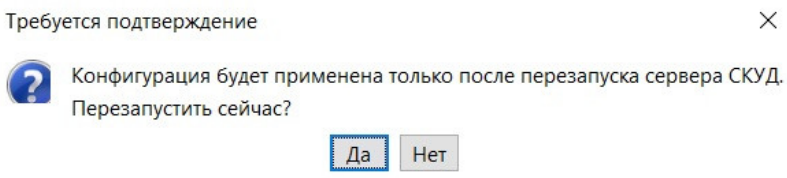
2. Указать путь к хранилищу сертификатов сервера Sigur. Для этого нужно перейти на вкладку «Безопасность» ПО «Управление сервером», развернуть

выпадающий список «Тип хранилища» и выбрать вариант «Файл PKCS#12». Далее необходимо указать путь к файлу формата .p12 или .pfx и пароль к нему в одноименных полях.



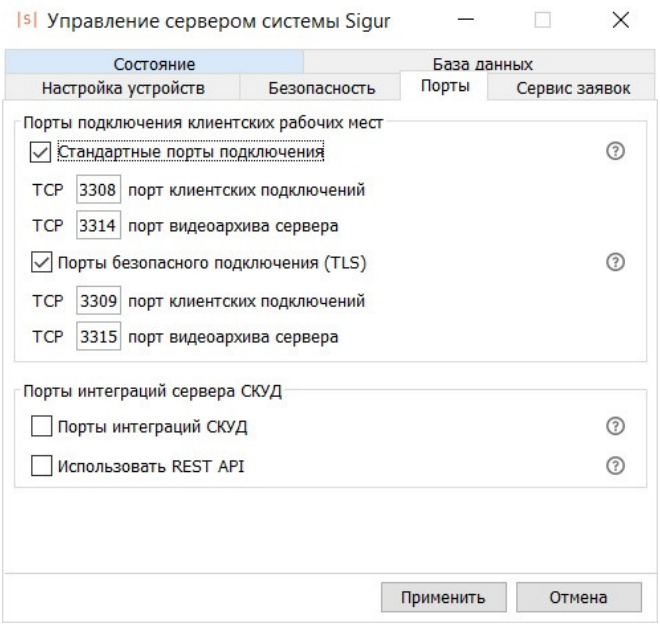
Вкладка «Безопасность» ПО «Управление сервером».

3. Далее нужно нажать кнопку «Применить», после чего система выведет предупреждение о необходимости перезапуска серверного модуля для применения новой конфигурации. Перезапустите серверный модуль.



Предупреждение о необходимости перезапуска серверного модуля.

4. Указать порты для защищенного соединения. Для этого нужно перейти на вкладку «Порты» ПО «Управление сервером» и активировать чек-бокс «Порты безопасного подключения (TLS)». По умолчанию для зашифрованного подключения клиентских мест к серверу используется порт TCP 3309, а для безопасного получения кадров IP-камер из видеоархива – порт TCP 3315. Вы можете использовать значения по умолчанию или изменить их.



Вкладка «Порты» ПО «Управление сервером».

Порты, использующиеся системой, не должны дублироваться.

Если требуется перевести взаимодействие полностью на защищенный режим, то стандартные порты сервера нужно отключить (подробнее – в соответствующем разделе).

Сертификат сервера Sigur используется на всех портах, использующих TLS (порт подключения клиентских мест, порт доступа к базе данных, порт для запроса кадров IP-камер из видеоархива, порт для взаимодействия через REST API, порт для взаимодействия по интеграционному протоколу OIF).

5. По окончании настройки нужно нажать кнопку «Применить» и перезапустить серверный модуль.

На этом настройка серверной части ПО Sigur завершена.

14.2.2. Ограничения и требования к сертификатам сервера СКУД

В систему можно добавить хранилище сертификатов сервера стандарта PKCS#12 (файл с расширением *.p12 или *.pfx). Хранилище сертификатов должно содержать:

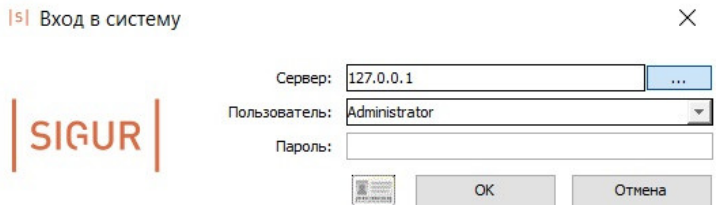
- Приватный ключ сервера. На текущий момент поддерживаются приватные ключи формата RSA и EC (в частности, тестировалось взаимодействие с prime256v1 и secp256v1). Минимальная длина ключа - 2048 бит.
- Валидный сертификат сервера формата X.509. Срок действия сертификата не должен быть истекшим.
- Цепочку доверия сертификатов формата X.509.

Сертификат сервера должен быть подписан последним центром сертификации в цепочке доверия.

14.2.3. Настройка клиентской части ПО Sigur

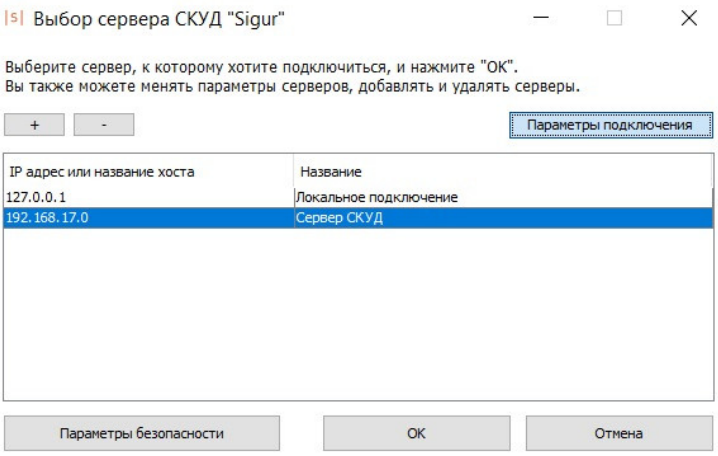
Требуется выполнить следующие настройки на каждом клиентском рабочем месте Sigur, которое будет устанавливать защищенное соединение с сервером:

1. Переключиться на использование зашифрованного соединения. Для этого необходимо запустить ПО «Клиент» и перейти в меню «Выбор сервера СКУД Sigur», нажав на кнопку «...» в стартовом меню «Вход в систему».



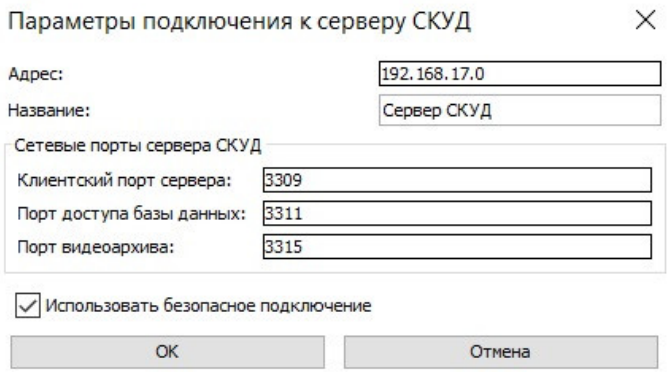
Меню «Вход в систему».

Далее необходимо ввести реквизиты соединения с новым сервером или выделить в списке ранее добавленный сервер и нажать кнопку «Параметры подключения».



Окно «Выбор сервера СКУД "Sigur"».

В окне «Параметры подключения к серверу СКУД» нужно активировать чек-бокс «Использовать безопасное подключение», при этом значения в блоке «Сетевые порты сервера СКУД» будут автоматически изменены. Убедитесь в том, что значения полей «Клиентский порт сервера» и «Порт видеоархива» (при необходимости) соответствуют ранее заданным номерам TCP-портов в ПО «Управление сервером». Для сохранения настроек необходимо нажать кнопку «ОК».



Окно «Параметры подключения к серверу СКУД».

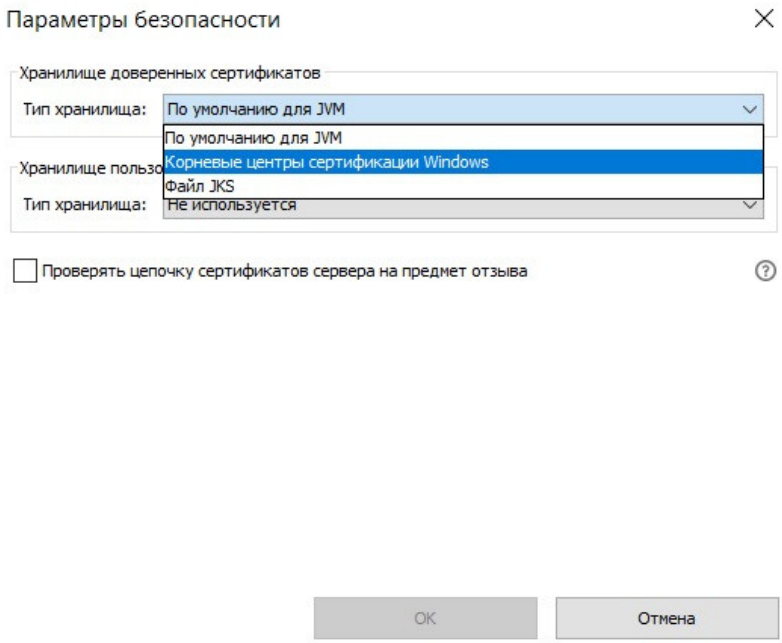
Настройка TCP-портов подключения производится отдельно для каждого сервера в списке. Параметры подключения к серверам хранятся локально на клиентском компьютере и являются уникальными для каждого пользователя ОС.

2. Определить хранилище доверенных центров сертификации для проверки сертификата сервера. Для этого необходимо нажать кнопку «Параметры безопасности» в меню «Выбор сервера СКУД Sigur» и выбрать из выпадающего списка «Хранилище доверенных сертификатов» нужный вариант.

Типы хранилищ отличаются для ОС Windows и Linux:

- **«По умолчанию для JVM (Java Virtual Machine)».** Доступно на ОС Windows и Linux. При выборе этой опции будут использоваться центры сертификации из каталога установки JVM или центры сертификации, указанные в параметрах запуска JVM.
- **«Корневые центры сертификации Windows».** Доступно на ОС Windows. В качестве хранилища доверенных сертификатов будет использовано системное хранилище ОС Windows. ПО Sigur просматривает как корневые сертификаты конкретного пользователя, так и корневые сертификаты для всей машины в целом.
- **«Файл JKS»**. Доступен на ОС Windows и Linux. Файл JKS (Java Key Store) должен содержать доверенные корневые сертификаты и должен быть создан утилитой keytool из состава JRE/JDK.
- **«Файл PKCS#12»**. Доступен на ОС Linux. Файл должен содержать доверенные корневые сертификаты и должен быть создан утилитой keytool из состава JRE/JDK.

Для сохранения настроек необходимо нажать кнопку «OK».



Окно «Параметры безопасности».

На этом настройка защищенного подключения со стороны клиентского рабочего места Sigur завершена.

Если сертификат сервера Sigur не будет подписан одним из центров сертификации в выбранном хранилище, то подключение будет прервано со стороны клиентской части ПО Sigur.

На вкладке «Параметры безопасности» также есть выпадающий список «Хранилище пользовательских сертификатов». Этот параметр используется для настройки функции взаимной аутентификации (подробнее – в разделе «Взаимная аутентификация»).

Хранилище доверенных центров сертификации должно быть сконфигурировано на каждом клиентском месте Sigur, которое использует защищенное подключение к серверу СКУД.

При корректной настройке системы соединение с сервером будет выполнено успешно. В противном случае пользователю будет выведено сообщение о невозможности подключения к серверу СКУД с указанием причины ошибки.

При использовании автоматического входа в Sigur (автологин) система оперирует параметрами подключения и безопасности пользователя операционной системы, от имени которого осуществляется вход.

Соответственно, клиентское рабочее место должно быть соответствующим образом сконфигурировано перед использованием автоматического входа в систему.

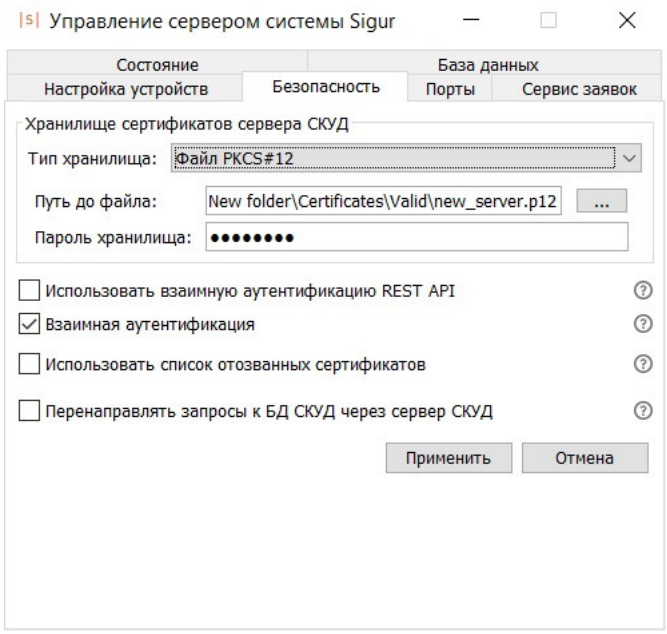
14.3. Взаимная аутентификация

В дополнение к проверке сертификата сервера возможно активировать функционал взаимной аутентификации. В этом случае все клиентские рабочие места, подключающихся по TLS, также предоставляют свой сертификат безопасности. В случае отсутствия сертификата клиента или его невалидности соединение будет прервано со стороны сервера Sigur.

Для настройки функционала взаимной аутентификации необходимо:

1. Сконфигурировать серверную часть Sigur аналогично инструкции в разделе «Настройка сервера Sigur».

2. Включить чек-бокс «Взаимная аутентификация» на вкладке «Безопасность» ПО «Управление сервером».



Чек-бокс «Взаимная аутентификация».

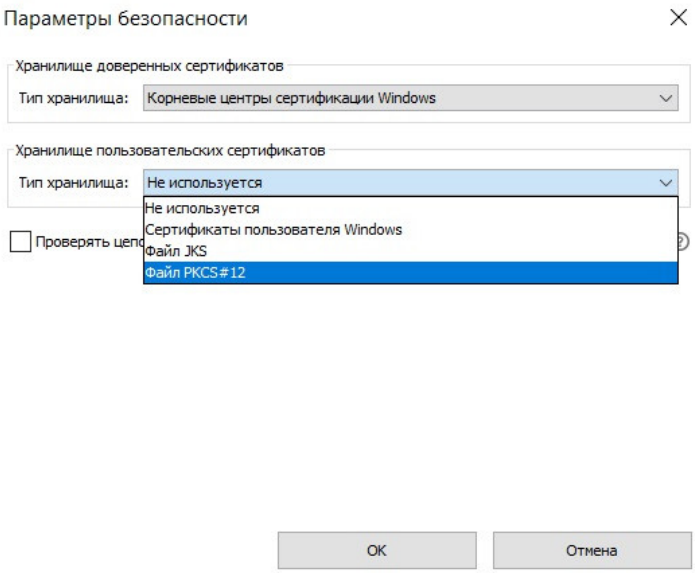
3. Применить настройки и перезапустить серверный модуль.

4. Сконфигурировать клиентское рабочее место согласно инструкции в разделе «Настройка клиентской части ПО Sigur».

5. Убедиться в том, что на клиентское место загружен сертификат безопасности, подписанный центром сертификации в цепочке доверия сервера. В меню ПО «Клиент» - «Выбор сервера СКУД Sigur» - «Параметры безопасности» необходимо выбрать хранилище клиентских сертификатов согласно

используемой ОС:

- **«Сертификаты пользователя Windows»**. Доступно на ОС Windows. В этом случае будут использованы личные сертификаты и приватные ключи из хранилища Windows.
- **«Файл JKS»**. Доступно на ОС Windows и Linux. Файл JKS должен содержать валидный сертификат клиента и его приватный ключ формата RSA/EC (в частности, тестировалось взаимодействие с prime256v1 и secp256v1). Файл должен быть создан утилитой keytool из состава JRE/JDK. Необходимо указать путь к файлу и пароль от хранилища.
- **«Файл PKCS#12».** Доступно на ОС Windows и Linux. Файл должен содержать валидный сертификат клиента и его приватный ключ формата RSA/EC (в частности, тестировалось взаимодействие с prime256v1 и secp256v1). Необходимо указать путь к файлу и пароль от хранилища.



Выбор хранилища пользовательских сертификатов при взаимной аутентификации.

При включении взаимной аутентификации сертификат клиента будет требоваться не только при подключении на порт клиентских рабочих мест, но и также при подключении на порт интеграции открытого интерфейса СКУД, если для него включена опция шифрования трафика.

14.4. Проверка статуса отзыва сертификата

В системе доступен функционал проверки того, был ли сертификат клиента или сервера Sigur отозван центром сертификации. Ниже описан процесс настройки обоих вариантов.

Проверка сервером Sigur статуса отзыва сертификата клиентского рабочего места.

Для этого в систему добавляется список отозванных сертификатов (CRL)

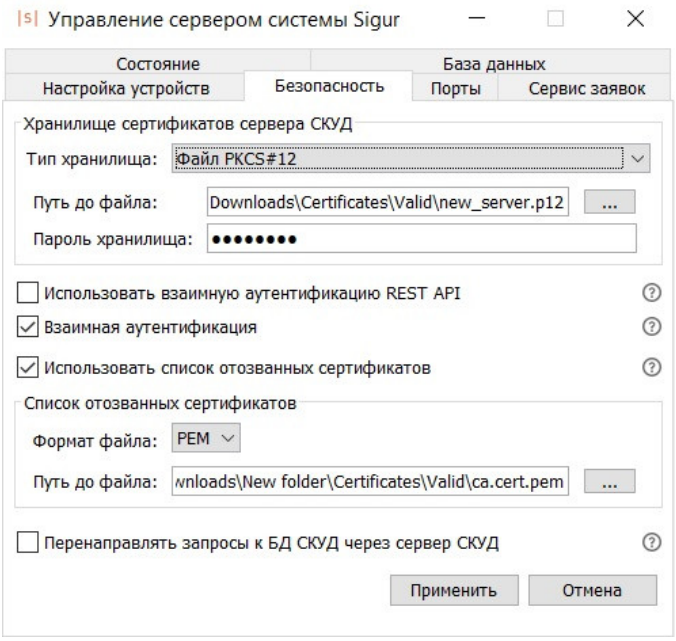
формата PEM или DER. Для активации функционала необходимо:

1. Включить чек-бокс «Взаимная аутентификация» на вкладке «Безопасность» ПО «Управление сервером».

2. Включить ставший доступным чек-бокс «Использовать список отозванных сертификатов».

3. После этого нужно выбрать из выпадающего списка нужный формат (PEM или DER) и указать путь до файла списка. Список отозванных сертификатов должен иметь валидный срок действия и должен быть подписан последним центром сертификации из цепочки доверия сервера СКУД.

4. После сохранения конфигурации сервера требуется перезапустить серверный модуль для того, чтобы новые настройки вступили в силу.



Настройка проверки сервером статуса отзыва сертификата клиентского рабочего места.

Клиентам с отозванными сертификатами будет запрещено подключаться к серверу СКУД на порты, использующие TLS. Если сертификат клиентского рабочего места содержится в этом списке, то TLS-соединение будет прервано сервером.

Проверка клиентом Sigur статуса отзыва сертификата сервера Sigur (или всей цепочки промежуточных сертификатов).

Клиентское рабочее место может использовать список отозванных сертификатов (CRL) или выполнять запрос к OCSP-серверу. Для активации функционала необходимо включить чек-бокс «Проверять цепочку сертификатов сервера на предмет отзыва» в меню ПО «Клиент» - «Выбор сервера СКУД Sigur» -

«Параметры безопасности». Далее становятся доступны следующие опции:

1. «Использовать точки распространения CRL». Система будет пытаться загружать CRL-файлы центров сертификации, если их URI указаны в сертификате сервера. URI должны быть явно прописаны в сертификате(сертификатах) сервера Sigur в атрибуте CRL Distribution Points X509v3 extension.

Пример:
crlDistributionPoints = URI:http://example.com/intermediate.crl.pem

Соединение будет прервано клиентом, если:

- Указанный атрибут отсутствует в сертификате сервера.
- Скачать CRL-файл не удалось.
- Один из проверяемых сертификатов цепочки отозван.

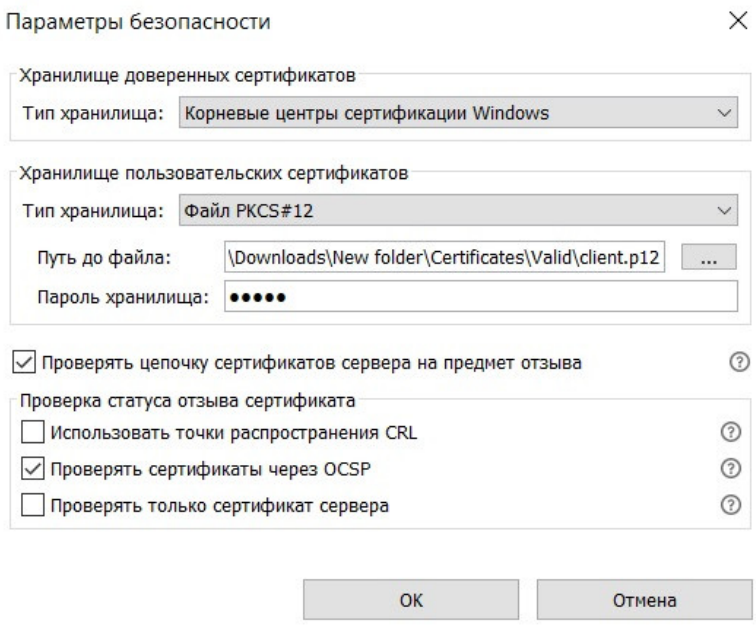
2. «Проверять сертификаты через OCSP». Предпочтительный вариант. Система будет отправлять запрос на OCSP-сервер для проверки отзыва сертификата сервера Sigur или цепочки сертификатов. URI OCSP-сервера должен быть явно прописан в атрибуте Authority Information Access X509v3 extension сертификата(сертификатов), предоставляемого сервером.

Пример:
authorityInfoAccess = OCSP;URI:http://ocsp.example.com

Соединение будет прервано клиентом, если:

- Указанный атрибут отсутствует в сертификате сервера.
- Один из проверяемых сертификатов цепочки отозван.
- Не удалось получить ответ от OCSP-сервера и опция «Использовать точки распространения CRL» отключена. В противном случае система дополнительно попытается получить CRL-файл.

3. «Проверять только сертификат сервера». Если опция отключена, то на предмет отзыва будет проверяться непосредственно сертификат сервера. Если опция активна, то будет проверяться вся цепочка доверия.



Настройка проверки клиентом Sigur статуса отзыва сертификата сервера Sigur и цепочки промежуточных сертификатов.

14.5. Безопасное подключение к базе данных Sigur

По умолчанию клиентские места Sigur получают информацию из базы данных СКУД, подключаясь к ней напрямую.

Вы можете активировать перенаправление трафика между клиентом и базой данных через сервер Sigur для обеспечения защиты персональных данных. Возможны следующие варианты конфигурации системы:

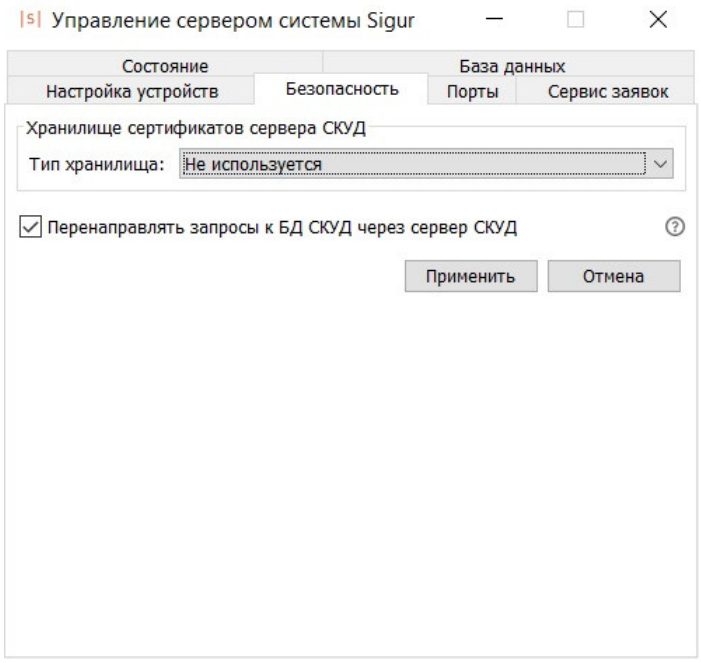
1. Перенаправлять запросы к БД через сервер без использования TLS-шифрования. Это исключает возможность прямого подключения клиентских мест к БД СКУД.
2. Перенаправлять запросы к БД через сервер совместно с шифрованием трафика по TLS. Таким образом обеспечивается максимальная защита данных в системе.

Функционал перенаправления трафика актуален только для подключений с клиентских рабочих мест ПО Sigur и не влияет на механизм работы интеграционных сервисов и веб-сервисов с БД Sigur.

Рассмотрим настройку перенаправления запросов к базе данных через сервер СКУД без использования шифрования.

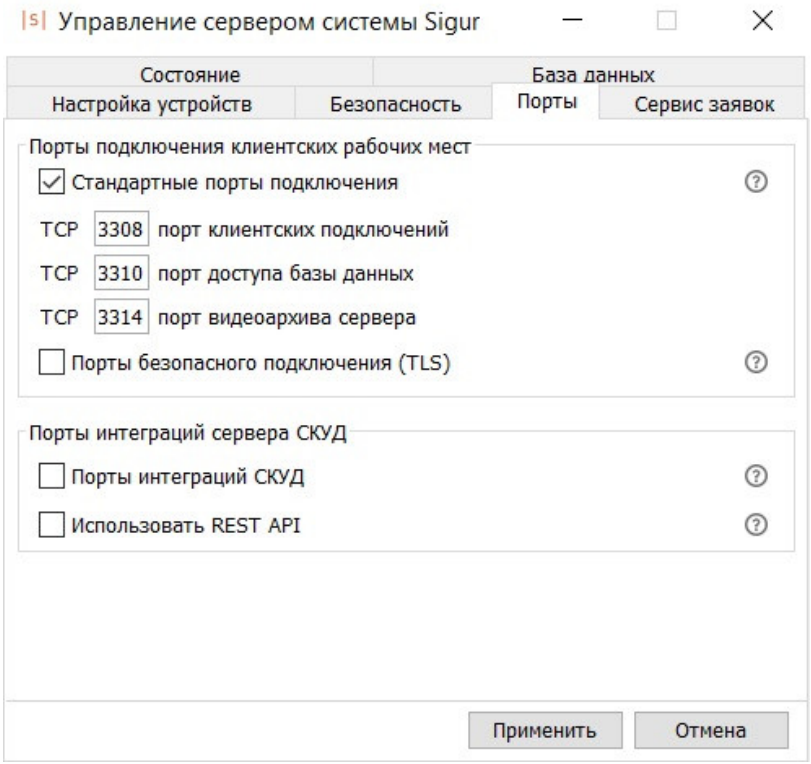
1. Конфигурирование серверной части Sigur:

- Включить чек-бокс «Перенаправлять запросы к БД СКУД через сервер СКУД» на вкладке «Безопасность» ПО «Управление сервером».



Активация функции «Перенаправлять запросы к БД СКУД через сервер СКУД».

- Сохранить изменения и перезапустить серверный модуль для того, чтобы для настройки стал доступен порт базы данных.
- Выбрать порт сервера для подключения клиентских мест к БД на вкладке «Порты» ПО «Управление сервером». По умолчанию используется порт TCP 3310. Вы можете использовать данное значение или изменить его. Перечень используемых системой портов указан в приложении.

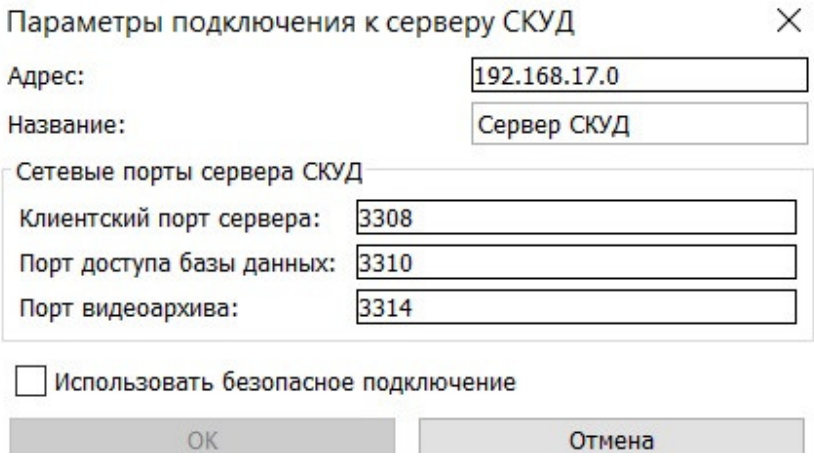


Выбор портов сервера при незащищённом соединении.

- Повторно сохранить настройки и перезапустить серверный модуль.

2. Конфигурирование клиентского рабочего места Sigur.

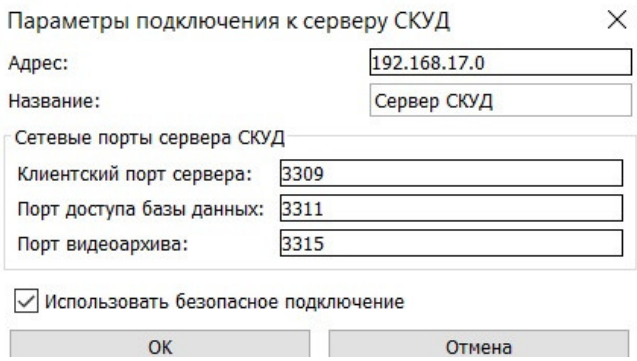
- Задать порт для подключения к базе данных в меню ПО «Клиент» - «Выбор сервера СКУД Sigur» - «Параметры подключения» - «Параметры подключения к серверу СКУД». Номер порта должен соответствовать порту, заданному ранее в настройках серверной части ПО.



Порты подключения к серверу при незащищённом соединении.

По завершении настройки клиентские рабочие места Sigur смогут подключаться к базе данных через сервер Sigur (без шифрования трафика).

В случае если требуется перенаправлять запросы к БД совместно с шифрованием по протоколу TLS, нужно дополнительно выполнить настройку сервера и клиентских рабочих мест аналогично инструкции в разделе «Установка зашифрованного соединения между клиентом и сервером». В этом случае для подключения к БД будет использоваться порт TCP 3311 (значение по умолчанию, номер порта доступен для изменения). Перечень используемых системой портов указан в приложении.



Порты подключения к серверу при защищённом соединении.

Функционал перенаправления запросов к базе данных также совместим с

опциями взаимной аутентификации и проверки статуса сертификата клиента или сервера.

Если в процессе запуска портов базы данных возникли какие-либо проблемы (например, порт уже занят), то система выведет соответствующее предупреждение в ПО «Клиент». Подробнее – в разделе «Диагностика состояния сетевых портов средствами ПО Sigur».

14.6. Шифрование взаимодействия по протоколам интеграции

Шифрование трафика по TLS также возможно использовать при подключении на порты интеграций сервера СКУД - порт REST API и порт интеграционного протокола OIF.

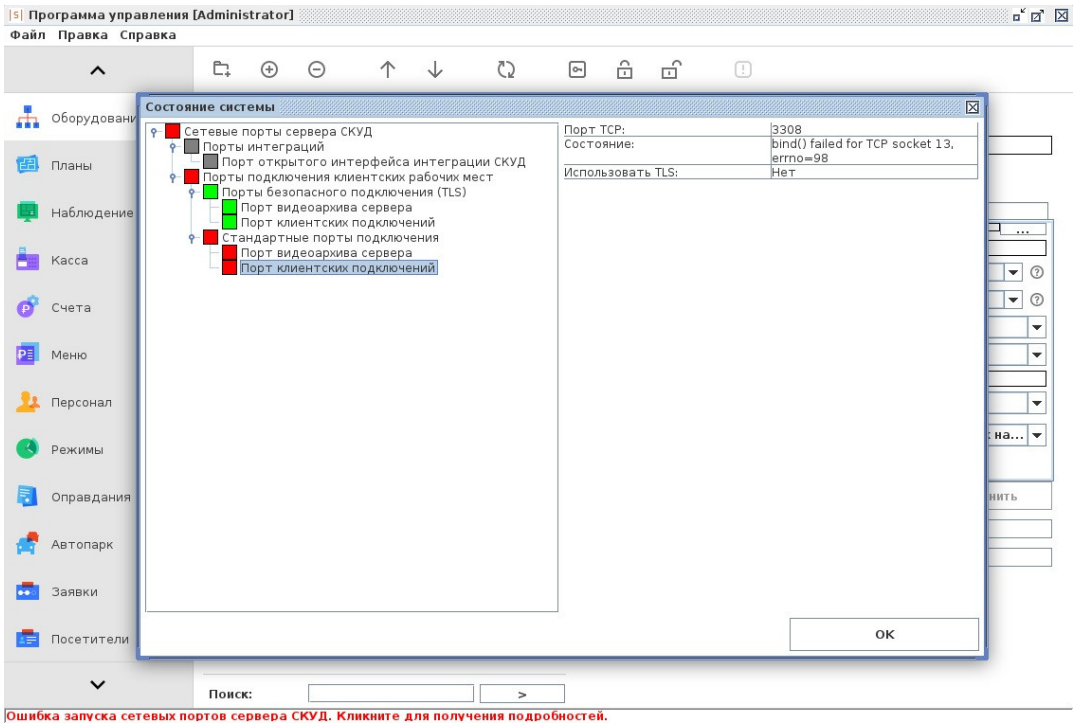
Информация о необходимых настройках размещена в отдельных руководствах для данных интеграций.

14.7. Диагностика состояния сетевых портов средствами ПО Sigur

Если какой-либо из портов сервера Sigur не может быть запущен, то в нижней части окна ПО «Клиент» будет выведено соответствующее предупреждение.

При нажатии на предупреждение открывается окно «Состояние системы», где отображается текущий статус сетевых портов сервера Sigur. Для просмотра подробной информации и сообщений об ошибках подключения необходимо выделить необходимый порт в списке. Для уточнения причины возникновения ошибки Вы можете обратиться в техническую поддержку Sigur.

На текущий момент в данном списке содержится информация о состоянии портов подключения клиентских рабочих мест и порта интеграции OIF.



Окно «Состояние системы».

Описание индикаторов состояния сетевых портов.

Цвет индикатора	Описание
Зеленый	Порт успешно запущен.
Серый	Порт отключен в настройках системы.
Красный	Неуспешная попытка запуска порта. См. текст ошибки в блоке «Состояние» в левой части окна.

15. Порты, используемые системой по умолчанию

Для связи между компонентами системы используется протокол TCP. Нижеприведённые таблицы содержат номера портов, используемых системой на стороне сервера по умолчанию.

TCP порты, используемые системой по умолчанию.

Номер порта		Для чего используется
Незашифрованное соединение	**Зашифрованное соединение (TLS)**	
3308	-	Для связи с NFC-терминалом.
3308	3309	Для связи с клиентскими местами.
3314	3315	Для передачи архивных кадров IP-камер на клиентские места.
3312	3312	Для предоставления доступа к серверу по протоколу открытого интерфейса (OIF).
9500	9500	Порт REST API.

Порт по умолчанию (подключение напрямую к БД)	Включено перенаправление запросов к БД через сервер Sigur		Для чего используется
	Незашифрованное соединение	**Зашифрованное соединение (TLS)**	
3305	3310	3311	Для клиентских подключений к серверу базы данных Sigur

UDP порты, используемые системой по умолчанию.

Номер порта	Для чего используется
3303	Для обмена управляющими сообщениями.
3305	Для информационного обмена с контроллерами без шифрования трафика.
3306	Для перевода контроллер в режим шифрования данных при взаимодействии с сервером.
3307	Для информационного обмена с контроллерами с шифрованием трафика (DTLS).

16. 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