SIGUR

Руководство администратора ПО Sigur

Редакция от 20.07.2026.

«Промавтоматика», г. Н. Новгород, 2026 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.

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 1.8.4.49 и версии микропрограммы контроллера 1.24.4.

Актуальная версия документа доступна на официальном сайте по ссылке.

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.
0004	13 марта 2024 г.	Актуализация в связи с выходом версии ПО 1.6.2.10. Обновление системных требований и порядка установки ПО Sigur на Debian и Red Hat Linux.
0005	04 сентября 2024 г.	Актуализация в связи с выходом версии ПО 1.6.3.14. Обновлены системные требования. Добавлены разделы «Управление сервером через командную строку (AdminCLI)», «Тип сервера БД», «Использование PostgreSQL в качестве сервера базы данных» и «Совместимость интеграций с ОС и СУБД». Также обновлены инструкции по установке ПО на Linux, об обновлении ПО, разделы с информацией об архитектуре сервера, управлении базой данных и добавлении/настройке IP-устройств. Актуализированы рекомендации по созданию сертификатов шифрования TLS в связи с поддержкой Java 17 версии. Отредактирована ссылка на скачивание драйвера ACR1252U.
0006	02 декабря 2024 г.	Добавлен раздел «Мониторинг состояния контроллера с использованием SNMP», также добавлена информация о портах, используемых системой по умолчанию при взаимодействии по SNMP.

Ревизия	Дата публикации	Что изменилось
0007	13 марта 2025 г.	Актуализация в связи с выходом версии ПО 1.6.4.53. Добавлен раздел «Тихая» установка и обновление на ОС Windows», содержащий информацию о новой опции для «тихой» установки сервера. Актуализирован раздел «Управление базой данных», в том числе, добавлены сведения о новом параметре «Статус серверных БД».
0008	21 апреля 2025 г.	Добавлен раздел «Шифрование трафика между сервером и контроллерами по DTLS».
0009	21 июля 2025 г.	В таблицу с перечнем интеграций и поддерживаемых для них ОС и СУБД добавлена информация об интеграции с устройствами Suprema. Добавлено уточнение о дате, выставляемой автоматически при удалении протоколов событий из БД. В системные требования к серверу СКУД добавлено указание на предпочтительное использование LTS-версий MariaDB.
0010	15 сентября 2025 г.	Актуализированы системные требования к серверу и клиентским рабочим местам. Актуализирована инструкция по созданию пользователя БД при установке ПО Sigur на Linux.
0011	16 октября 2025 г.	Актуализация в связи с выходом версии ПО 1.6.7.60. Обновлён раздел «Изменение IP-параметров устройства».
0012	19 декабря 2025 г.	Дополнена инструкция по обновлению ПО Sigur на Linux. Актуализирована информация о сбросе профиля шифрования контроллера.
0013	19 января 2026 г.	Актуализирован раздел «Системные требования СКУД Sigur»: добавлена информация о поддержке операционных систем РЕД ОС и РОСА «Хром».
0014	13 февраля 2026 г.	Актуализировано наименование пакета веб-сервисов для Debian в инструкциях по установке и обновлению ПО.

Ревизия	Дата публикации	Что изменилось
0015	21 апреля 2026 г.	Добавлена инструкция по предварительной установке драйверов для считывателя MR100 USB. Добавлена информация о расположении видеоархива в ОС Linux и требованиях к правам доступа при использовании пользовательской директории. Добавлено описание смены профиля шифрования DTLS без передачи приватного ключа по незащищённому каналу. Добавлено описание использовании цепочки CA-сертификатов в профиле шифрования DTLS. Добавлено описание настройки DNS и FQDN сервера СКУД в IP-конфигурации контроллера. Добавлено описание поддержки аутентификации контроллеров по протоколу EAP-TLS (IEEE 802.1X). Обновлена информация об использовании PostgreSQL в качестве сервера базы данных Sigur, а также добавлена информация о настройке схем и наименований БД сервера и веб-сервисов. В раздел «Управление сервером через командную строку (AdminCLI)» добавлена информация о командах setMutualAuthRest, restStatus, а также о новых командах для управления БД: init, setSchema, changeServiceDbName, changeServiceDbSchema. Добавлены новые разделы Roles и CentralServer. В инструкциях по установке ПО Sigur и резервированию БД на ОС Linux добавлена информация о новой БД SYNC. Актуализирован путь установки ПО Sigur на ОС Windows. Обновлены системные требования при использовании встроенного распознавания лиц. Добавлены разделы «Особенности обновления на версии ПО 1.8.x.x» и «Нагрузочные характеристики системы Sigur». В раздел «Совместимость интеграций с ОС и СУБД» добавлена информация об интеграциях со считывателями BioSmart (4,5, WTC2, PV-WTC), BioSmart PalmJet и устройствами хранения ECOS.

Ревизия	Дата публикации	Что изменилось
0016	10 июня 2026 г.	Добавлен раздел «Оптимизация работы сервера с контроллерами». Актуализирован раздел «Настройка IP-устройств» согласно функциональности ПО версии 1.8.4.35 и версии микропрограммы контроллера 1.24.1, в т. ч. добавлена информация про работу с DNS-серверами и обновлена инструкция по получению сетевых параметров от DHCP-сервера. Добавлена информация об ограничениях ввода пароля контроллера. Актуализирован раздел «Шифрование трафика между сервером и контроллерами по DTLS». Актуализирована информация о рекомендуемых характеристиках производительности локального сервера в рамках разных пакетов лицензирования. Актуализирована информация о команде update утилиты AdminCLI.
0017	09 июля 2026 г.	Добавлено упоминание возможности настроить сетевые параметры контроллеров с помощью утилиты «DCT».
0018	20 июля 2026 г.	Обновлён раздел «Основные принципы работы системы Sigur»: добавлена информация о центральном сервере, описание связи локального сервера с центральным.

3. Используемые определения, обозначения и сокращения

СКУД	Система контроля и управления доступом. Программно–аппаратный комплекс, предназначенный для осуществления функций контроля и управления доступом.
Центральный сервер	Сервер, который является единой точкой управления СКУД Sigur. Главный источник кадровой информации и верхнеуровневых политик безопасности системы.
Локальный сервер	Любой сервер Sigur, который расположен на конкретном объекте или в филиале системы и обеспечивает выполнение задач СКУД в своей зоне ответственности.
Глобальный персонал	Объекты доступа, которые создаются и управляются через центральный сервер.
Локальный персонал	Объекты доступа, которые создаются и управляются на локальном сервере.
Точка доступа	Место, где осуществляется контроль доступа. Например: дверь, турникет, ворота, шлагбаум, оборудованные считывателем, электромеханическим замком и другими необходимыми средствами.
Объект доступа	Сотрудник, посетитель, автомобиль или другое транспортное средство, действия которого регламентируются правилами разграничения доступа.
Режим доступа	Последовательность дней с заданной датой начала, определяющая интервалы разрешения доступа и рабочие графики персонала. Используется для настройки правил прохода, учёта рабочего времени и автономной работы точек доступа.
ПО	Программное обеспечение.
БД	База данных.
СУБД	Система управления базами данных.
ПК	Персональный компьютер.

4. Основные принципы работы системы Sigur

4.1. Обзор компонентов

СКУД Sigur состоит из следующих компонентов:

- **Центральный сервер** – компьютер под управлением операционной системы Linux Debian, Ubuntu, RHEL, CentOS с установленным программным обеспечением Sigur Центральный сервер. Обеспечивает централизованное управление персоналом и правами доступа для всех подключённых локальных серверов. См. подробные сведения в «Руководстве по настройке и использованию ПО Sigur Центральный сервер».

- **Локальный сервер** (далее – сервер) – компьютер под управлением операционной системы Windows, Linux Debian, RHEL, CentOS, Fedora, Astra Linux, РЕД ОС или РОСА «Хром» с установленным программным обеспечением Sigur. Обеспечивает функционирование СКУД на конкретном объекте, управляет контроллерами, осуществляет сбор и хранение событий. Может работать автономно или подключаться к центральному серверу для синхронизации данных.

- **Клиентское место** – рабочее место пользователя системы, которое можно запустить на любом компьютере под управлением операционной системы Windows, Linux Debian, RHEL, CentOS, Fedora, Astra Linux, РЕД ОС или РОСА «Хром», связанном с локальным сервером по протоколу TCP/IP, или непосредственно на локальном 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 RS-485 (модели с префиксом R), а также к считывателям, датчикам и исполнительным устройствам. Контроллер Sigur является сетевым контроллером с полностью автономным алгоритмом принятия решений и их регистрации. Независимо от наличия или отсутствия связи с сервером, 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 Sigur Connect** – электронный модуль в пластиковом корпусе. Обеспечивает преобразование сигналов стандартного порта USB в стандартный порт RS-485. Используется для подключения к серверу контроллеров R-серии. К одному серверу можно подключить до 16 преобразователей, получая структуру линии связи типа

«звезда». Линия связи RS-485 соединяет преобразователи с контроллерами. К каждой линии можно подключить до 255 контроллеров. Возможно использование повторителей, увеличивающих максимальную длину линии связи в два или четыре раза.

- **Мобильный терминал Sigur** – любой смартфон или планшет на базе ОС Android или РЕД ОС М с поддержкой NFC или OTG и установленным приложением «Мобильный терминал Sigur». 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. Возможны два варианта работы терминала – Online (постоянная связь с сервером) и Offline (автономная работа без связи с сервером, зафиксированные события хранятся во внутренней памяти устройства до восстановления 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.

- **Настольный считыватель** – используется для оперативного поиска сотрудников в базе данных и для быстрого ввода кода нового пропуска в систему. Поддерживаются считыватели:

  - Sigur MR100 USB (для карт Mifare, EM-Marine, HID ProxCard II);
  - Sigur Reader-EH (для карт EM-Marine и HID ProxCard II);
  - IronLogic Z-2 USB (для карт EM-Marine, HID ProxCard II и Mifare в режиме чтения UID);
  - ACR1252U (для карт Mifare);
  - ESMART DUAL USB (для карт Mifare, требует наличия лицензии),
  - а также подключение любых считывателей с выходным интерфейсом Wiegand-26 к адаптеру Sigur Reader-W (для прочих форматов карт).

  Для добавления биометрических шаблонов могут использоваться:
  - Biosmart FS-80;
  - Biosmart DCR-PV;
  - BioSmart AirPalm:
  - Anviz U-Bio;
  - ВЗОР-Enroll.

- **IP-камеры** – подразумевается установка камер около исполнительных устройств (опционально). Камеры могут быть подключены к серверу Sigur по IP-сети для трансляции живого видео и накопления фотоархива по факту происходящих на исполнительных устройствах событий, фиксируемых на сервере СКУД. Альтернативно может быть настроена интеграция с серверами систем видеонаблюдения.

- Дополнительная компьютерная периферия, подключаемая (опционально) к клиентскому месту:

  - **web-камеры** – для оперативного занесения фотографий объектов доступа;
  - **сканеры** – для сканирования и добавления изображений к объектам доступа, для распознавания персональной информации при выдаче пропуска посетителю (требуется лицензия);
  - **принтеры** – для печати информации в результате работы некоторых дополнительных функций ПО Sigur.

4.2. Принципы работы системы Sigur

4.2.1. Сервер

Сервер Sigur представляет собой компьютер под управлением операционной системы Windows, Linux Debian, RHEL, CentOS, Fedora, Astra Linux, РЕД ОС или РОСА «Хром» с установленным программным обеспечением Sigur.

Программное обеспечение сервера состоит из двух программных модулей:

- Сервер базы данных – предоставляет доступ компонентам системы к базе данных.
- Серверный модуль – обеспечивает информационный обмен с контроллерами по линии связи. В состав серверного модуля также входят веб-сервисы, которые обеспечивают функционирование веб-интерфейса для работы с пропусками посетителей и REST-интерфейса.

4.2.2. Контроллер

Контроллер Sigur является сетевым контроллером с полностью автономным алгоритмом принятия решений и их регистрации.

Независимо от наличия или отсутствия связи с сервером, контроллер принимает решение о запрете или разрешении доступа, реакции на изменения состояния внешних датчиков и т. д. самостоятельно, на основании автономной базы ключей и режимов доступа. Произошедшее событие регистрируется также автономно, с указанием даты и времени встроенных часов реального времени. На сервер передаётся лишь информация о принятом решении.

Все ключи, режимы и события хранятся в энергонезависимой памяти контроллера (FLASH и FRAM).

Особенности работы контроллера:

- Время принятия контроллером решения о разрешении/запрете доступа не превышает 5 миллисекунд.
- Текущая работа контроллера не зависит 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 сервера со всеми контроллерами). 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.

Настройки, определяющие свойства подключённых датчиков, считывателей и исполнительных устройств, а также разграничения уровней доступа осуществляются с помощью программного обеспечения Sigur.

4.2.3. Связь с центральным сервером

Локальный сервер может быть подключён к центральному серверу Sigur. При подключении на сторону центрального сервера синхронизируются данные о локальном персонале, точках доступа, зонах, профилях чтения идентификаторов и события проходов. С центрального сервера на локальный передаются данные о глобальном персонале и их правах доступа. При отсутствии связи с центральным сервером локальный сервер продолжает работать автономно.

Локальные серверы взаимодействуют только с центральным сервером и не взаимодействуют друг с другом напрямую. Подробнее о настройке подключения к центральному серверу см. в «Руководстве по настройке и использованию ПО Sigur Центральный сервер».

4.2.4. Связь сервера с контроллерами

В штатном режиме сервер 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 контроллерам раз в 30 секунд.

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

4.2.5. Оптимизация работы сервера с контроллерами

Сервер Sigur обрабатывает взаимодействие с контроллерами в двух независимых очередях задач: очереди обмена данными и очереди синхронизации. По умолчанию каждая очередь работает в один поток. Этого режима достаточно для большинства объектов.

При большом количестве подключённых контроллеров (более 5000 точек доступа) и высоком объёме операций обмена и синхронизации может возникнуть нехватка производительности. В таких случаях однопоточной обработки становится недостаточно, что может проявляться в виде:

- задержек при обработке событий от контроллеров;
- замедления синхронизации устройств;
- ошибок при обновлении прошивки контроллеров или применении конфигурации.

Для решения подобных проблем в системе предусмотрена возможность оптимизации производительности за счёт использования многопоточности.

Функция расширенной оптимизации производительности доступна только при наличии лицензии Enterprise. На лицензиях ниже уровня Enterprise настройка многопоточности недоступна, сервер работает в автоматическом режиме.

Настройка многопоточности выполняется только специалистом технической поддержки Sigur. Самостоятельное изменение конфигурационных файлов не рекомендуется.

4.3. Ключевые элементы базы системы Sigur

4.3.1. Список точек доступа СКУД с их настройками

В списке содержатся все подключённые 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, используемые для задания правил доступа, интервалов рабочего времени объектов доступа, а также режимы автономной работы точек доступа. Режим представляет собой последовательность дней (от 1 до 32) 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» ПО «Клиент». 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 Sigur 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 ПО Sigur

При работе с большими базами данных (большое количество сотрудников и точек доступа) рекомендуется выбирать Linux-дистрибутивы в качестве операционной системы. Программное обеспечение Sigur на Linux использует 64-битную архитектуру. Установка серверной части ПО Sigur на Linux обеспечивает более высокую производительность и стабильность системы, улучшенную безопасность и гибкий контроль, включая управление сервером через командную строку.

Обратите внимание, что при работе Sigur с функциями видеонаблюдения (трансляцией живого видео, 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. Требования к операционной системе

Установка сервера и клиентских рабочих мест Sigur производится на компьютеры под управлением 64-разрядных операционных систем Windows, Linux Debian, RHEL, CentOS, Fedora, Astra Linux, РЕД ОС и РОСА «Хром». Поддерживаемые версии операционных систем перечислены в данном разделе.

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.

5.2. Рекомендуемая конфигурация сервера

- ОС: только 64-разрядные Windows 10 / Windows Server 2019 / Linux Debian 11 / RHEL 9 (с последним пакетом обновлений) / CentOS 8 / Fedora 35 / Astra Linux 1.8 / РЕД ОС 7.3 / РЕД ОС 8 / РОСА «Хром» 12 Сервер.
- Процессор: уровня Intel Core i7 и выше (8 ядер).
- Память: не менее 16 Гб.
- Свободное место на жёстком диске: 250 Гб.
- Сервер БД (на Linux):
    - MariaDB версии 10.7.2 и выше. Рекомендуется использовать версии с долгосрочной поддержкой (LTS). Обратите внимание: начиная с версии 11.4.x в MariaDB по умолчанию используются защищённые соединения (SSL/TLS). В текущей версии ПО Sigur такой режим работы не поддерживается. При использовании MariaDB 11.4.x и выше необходимо вручную отключить SSL/TLS в конфигурации сервера базы данных.
    - PostgreSQL версии 13 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).

5.3. Минимальная конфигурация сервера

- ОС: только 64-разрядные Windows 10 / Windows Server 2016 / Linux Debian 11 / RHEL 8 (с последним пакетом обновлений) / CentOS 8 / Fedora 35 / Astra Linux 1.8 / РЕД ОС 7.3 / РЕД ОС 8 / РОСА «Хром» 12 Сервер.
- 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.
- Сервер БД (на Linux): MariaDB версии 10.7.2 и выше, либо PostgreSQL версии 13 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).

5.4. Требования при использовании встроенного распознавания лиц

Встроенное распознавание лиц Sigur не поддерживается на сервере под управлением ОС RHEL / РЕД ОС / РОСА «Хром».

При использовании встроенной функции распознавания лиц необходимо руководствоваться рекомендуемыми системными требованиями к серверу, т. к. данная функция требует значительно больших ресурсов. Например, обработка одного кадра на одном ядре Intel Core i5-7260U@2.2GHz составляет около 150 мс (т. е. около 26 кадров в секунду на 4-ядерном процессоре). Однако значение варьируется в зависимости от размера кадра, модели процессора и ряда других параметров.

Для корректной работы распознавания лиц при использовании сервера СКУД в виртуальной среде необходимо, чтобы конфигурация виртуальной машины имела доступ к набору инструкций процессора SSE4.2.

В случае Windows рекомендуется использовать 64-разрядную версию ПО Sigur.

5.5. Рекомендуемая конфигурация клиентского места

- ОС: только 64-разрядные Windows 10 / Linux Debian 11 / RHEL 8 / CentOS 8 / Fedora 35 / Astra Linux 1.8 / РЕД ОС 7.3 / РЕД ОС 8 / РОСА «Хром» 12 Рабочая станция.
- Процессор: уровня Intel Core i3 и выше, не менее 4 ядер на частоте 3 ГГц.
- Память: не менее 8 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.

5.6. Минимальная конфигурация клиентского места

- ОС: только 64-разрядные Windows 10 / Linux Debian 11 / RHEL 8 / CentOS 8 / Fedora 35 / Astra Linux 1.8 / РЕД ОС 7.3 / РЕД ОС 8 / РОСА «Хром» 12 Рабочая станция.
- 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.

5.7. Нагрузочные характеристики системы Sigur

Сервер Sigur поддерживает следующие рекомендуемые характеристики производительности одного локального сервера (в зависимости от выбранного пакета лицензирования):

Рекомендуемые характеристики производительности	**Pro**	**Enterprise**
Количество подключённых контроллеров	250	2 000
Количество клиентских рабочих мест	50	200
Количество точек доступа на один сервер	1 000	10 000
Количество объектов доступа (идентификаторов)	10 000	100 000
Количество одновременно работающих мобильных терминалов в офлайн-режиме	15	
Количество мобильных терминалов в офлайн-режиме при подключении к серверу	50	

Рекомендуемые характеристики производительности	Pro	Enterprise
Количество поддерживаемых камер в режиме распознавания	• FullHD, ALG1 — 4 камеры; • FullHD, ALG2 — 2 камеры.	

При превышении одного или нескольких указанных параметров необходимо произвести дополнительную оценку архитектуры решения. В таких случаях рекомендуется рассмотреть внедрение центрального сервера или использование лицензии Enterprise для локального сервера.

Данные характеристики являются максимально допустимыми при соблюдении рекомендуемых требований к аппаратному обеспечению сервера.

5.8. Совместимость интеграций с ОС и СУБД

Совместимость с операционными системами.

Интеграция	Операционная система				
	Windows	Linux Debian	RHEL	РОСА «Хром»	РЕД ОС
KeyGuard	✓	✓	✓	✓	✓
Промет	✓	✓	✓	✓	✓
TrueIP	✓	✓	✓	✓	✓
BAS-IP	✓	✓	✓	✓	✓
Hikvision (распознавание лиц)	✓	✓	✓	✓	✓
Hikvision (тепловизоры)	✓	✓			
BioSmart (4,5, WTC2, PV-WTC)	✓	✓	✓		
BioSmart Quasar	✓	✓			
BioSmart PalmJet	✓	✓	✓		
ZKTeko	✓	✓			
HikCentral	✓	✓			
Domination Auto	✓	✓			
Beward	✓	✓			

Интеграция	Операционная система				
	Windows	Linux Debian	RHEL	РОСА «Хром»	РЕД ОС
Suprema	✓	✓	✓		
ECOS	✓	✓	✓		

Совместимость с СУБД.

Интеграция	СУБД	
	MariaDB	PostgreSQL
KeyGuard	✓	✓
Промет	✓	✓
TrueIP	✓	✓
BAS-IP	✓	✓
Hikvision (распознавание лиц)	✓	✓
Hikvision (тепловизоры)	✓	
BioSmart (4,5, WTC2, PV-WTC)	✓	
BioSmart Quasar	✓	
BioSmart PalmJet	✓	✓
ZKTeko	✓	
HikCentral	✓	✓
Domination Auto	✓	✓
Beward	✓	
Suprema	✓	✓
ECOS	См. информацию ниже.	

Для интеграции с устройствами хранения ECOS поддержка СУБД зависит от операционной системы:

- Windows – интеграция работает с MariaDB;
- Linux – интеграция работает с PostgreSQL.

6. Архитектура серверного программного обеспечения

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

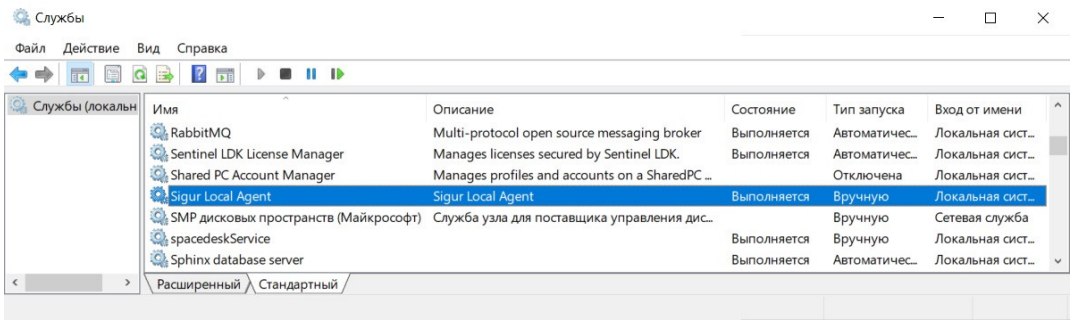
Сервер базы данных предоставляет доступ компонентам системы к базе данных.

Серверный модуль реализует функциональность СКУД, обеспечивает информационный обмен с контроллерами по линии связи и работу интеграций. В состав серверного модуля, в числе прочего, входит набор веб-сервисов, которые обеспечивают работу веб-интерфейса для работы с пропусками посетителей и REST-интерфейса.

Компоненты сервера запускаются автоматически при загрузке операционной системы.

ОС Windows.

Для управления компонентами сервера Sigur, как правило, используется программа «Управление сервером», возможности которой описаны в данном руководстве. Также может быть использована стандартная утилита Windows «Службы».



Управление службами системы с помощью утилиты «Службы».

Службы, используемые сервером Sigur на ОС Windows:

- Sphinx database server – сервер базы данных;
- Sigur Local Agent – служба, контролирующая работу процессов сервера;
- RabbitMQ – служба для установления связи между компонентами системы.

Когда сервер Sigur запущен, в операционной системе работают следующие процессы:

- mysqld.exe;

- local-agent.exe;
- sphinxd.exe – серверный процесс Sigur;
- процессы OpenJDK – процессы, отвечающие за работу веб-сервисов Sigur.

ОС Linux.

Для управления компонентами сервера можно использовать программу «Управление сервером», а также утилиту командной строки AdminCLI.

Сервером Sigur используется служба (демон) local-agent.service, контролирующая работу процессов сервера СКУД. В операционной системе активен процесс local-agent и его дочерние процессы, включая веб-сервисы и сервер.

Сервером Sigur также используются служба и процессы сервера базы данных.

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 программным компонентам Sigur к 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 Sigur.

7.1. Установка системы Sigur

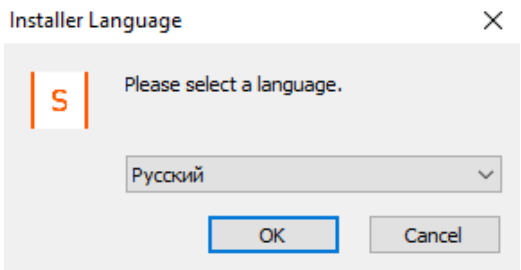
7.1.1. ОС Windows

Для установки программного обеспечения Sigur:

1. Войдите в операционную систему с правами администратора.

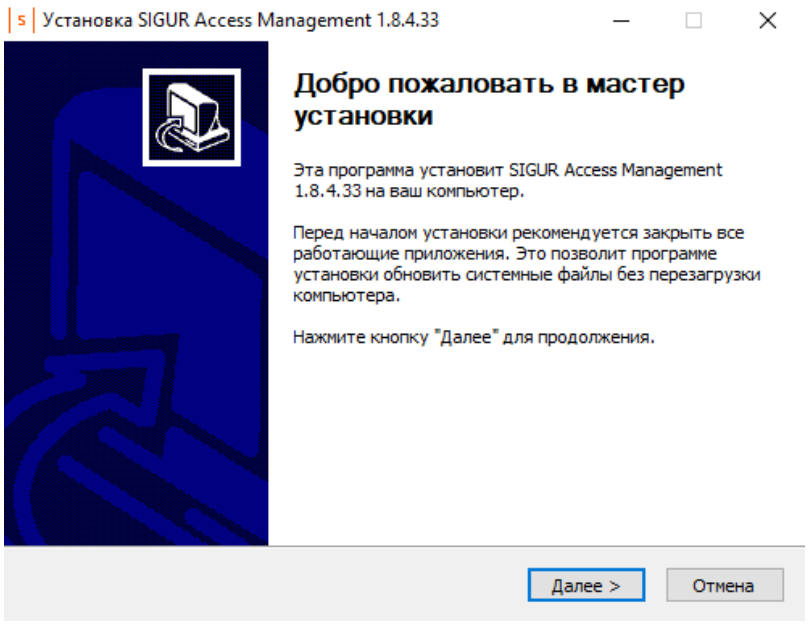
2. Запустите файл setup-XX.exe (где XX – номер версии устанавливаемого ПО).

3. Выберите язык интерфейса программы.



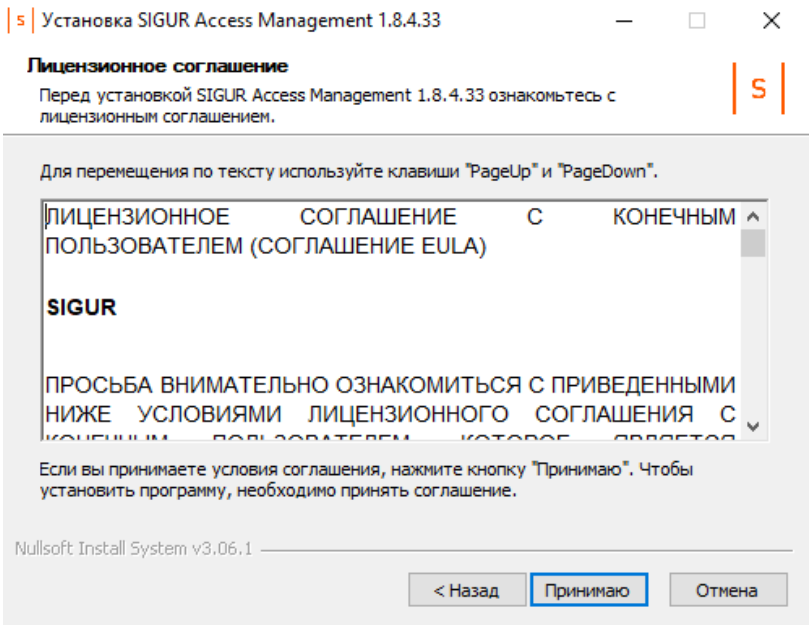
Выбор языка.

4. Откроется окно мастера установки. Нажмите «Далее».



Мастер установки.

5. Ознакомьтесь с условиями лицензионного соглашения и нажмите «Принимаю».

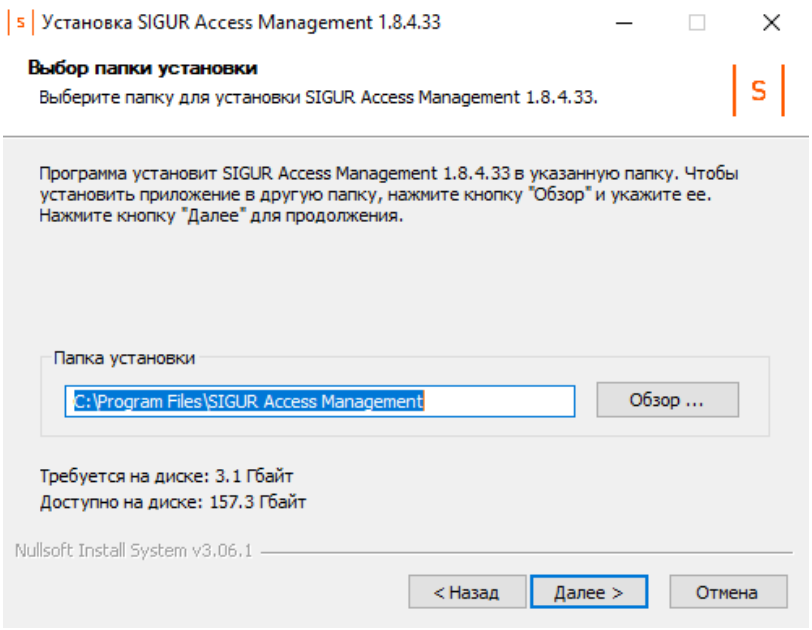


Лицензионное соглашение.

6. Выберите папку для установки программы. По умолчанию установка происходит в папку:

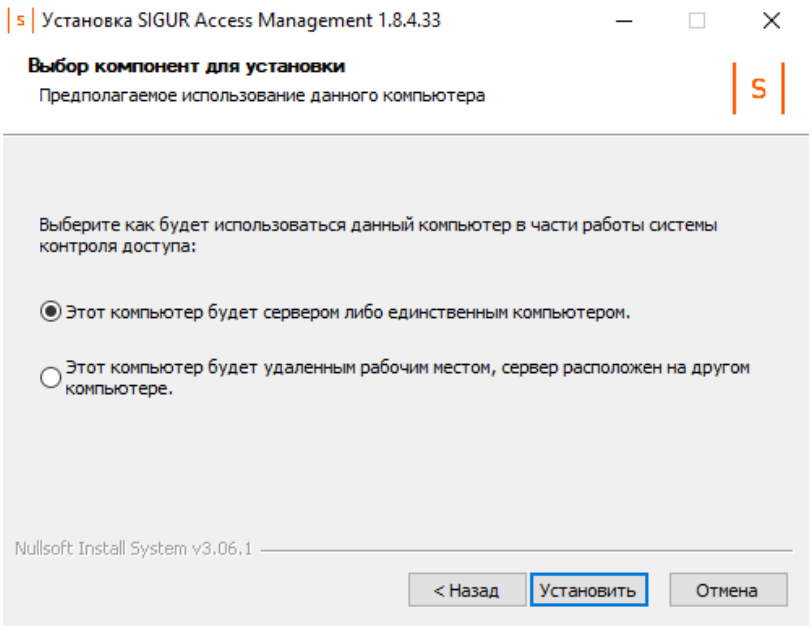
- C:\Program Files (x86)\SIGUR access management\ (для 32-разрядной версии);
- C:\Program Files\SIGUR access management\ (для 64-разрядной версии).

При необходимости можно изменить путь установки, нажав кнопку «Обзор».



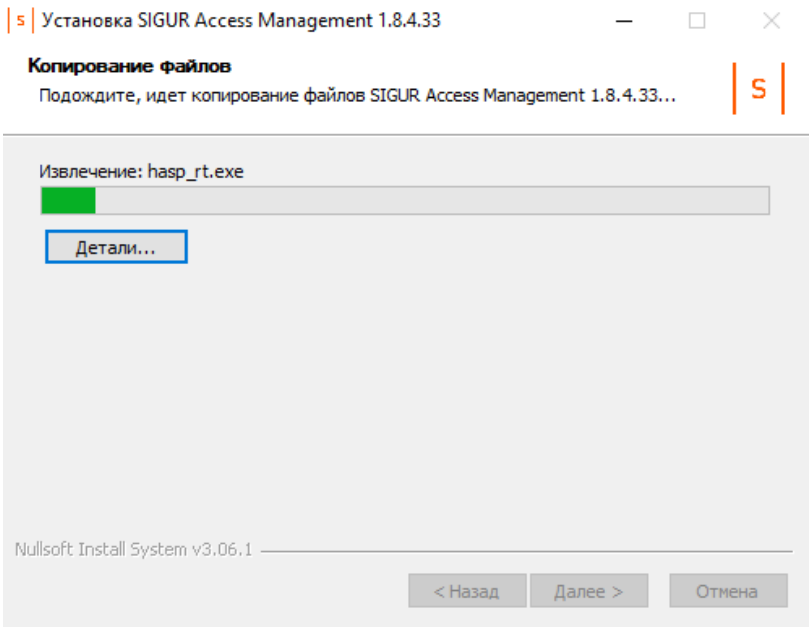
Выбор папки программы.

7. Выберите тип установки. Отметьте нужный вариант и нажмите «Установить».



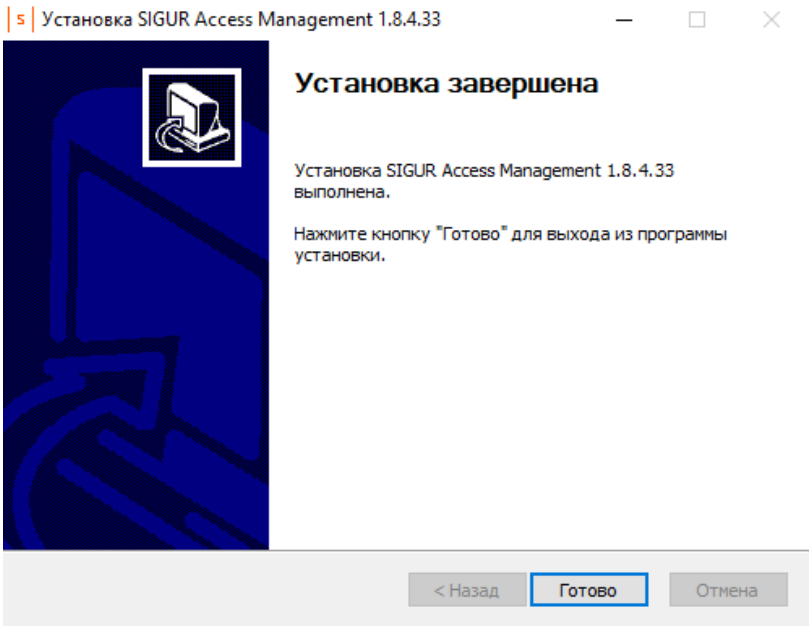
Выбор типа установки.

8. Откроется окно «Копирование файлов», в котором будет отображаться процесс установки программы.



Процесс установки.

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



Завершение работы мастера установки.

7.1.2. «Тихая» установка и обновление на ОС Windows

При необходимости проведения «тихой» установки или обновления администраторы компании могут использовать соответствующие ключи инсталлятора:

- /S – при установке с нуля выполняет установку клиентского рабочего места ПО Sigur.
- /S – при обновлении обновляет уже установленное ПО, сохраняя его тип (сервер обновляется как сервер, клиент – как клиент).
- /S /SERVER – выполняет установку сервера в тихом режиме. При обновлении ключ /SERVER игнорируется.

7.1.3. ОС Linux

Порядок установки ПО Sigur:

1. Установка зависимостей.

Для корректной работы системы Sigur требуются утилиты sudo и openssl, а также Java 17 версии.

1.1. Утилита sudo.

Для проверки того, есть ли на сервере утилита sudo, введите в командную строку наименование утилиты:

sudo

В случае отсутствия утилиты вы увидите соответствующее сообщение. Для установки воспользуйтесь командой:

Linux Debian	*apt install sudo*
RHEL	*yum install sudo*

1.2. Утилита openssl.

Для проверки версии openssl воспользуйтесь командой:

openssl version

В случае отсутствия утилиты вы увидите соответствующее сообщение.

Установить утилиту можно командой:

Linux Debian	*sudo apt install openssl*
RHEL	*sudo yum install openssl*

1.3. Java 17.

Для успешной установки и работы серверной части ПО Sigur требуется Java 17. Проверить версию Java можно командой:

java -version

Для установки Java 17 можно воспользоваться командами:

Linux Debian	*sudo apt update* *sudo apt install openjdk-17-jre*
RHEL	*sudo dnf check-update* *sudo dnf install java-17-openjdk*

Скачать файлы также можно, перейдя по данной ссылке.

2. Установка и настройка базы данных.

Система Sigur может использовать MariaDB или PostgreSQL в качестве сервера базы данных. Данная инструкция содержит рекомендации по настройке БД MariaDB. Подробнее об использовании PostgreSQL в Sigur – см. соответствующий раздел.

2.1. Стандартная настройка БД.

2.1.1. Установите сервер MariaDB.

Linux Debian	*sudo apt-get install mariadb-server*
RHEL	*sudo yum install mariadb-server*

2.1.2. Для корректной работы сервисов системы необходимо отключить чувствительность к регистру в настройках сервера MariaDB.

Это можно сделать, отредактировав параметр lower_case_table_names. Этот текстовый параметр может содержаться в одном из файлов конфигурации сервера БД в каталоге /etc/mysql/*. Имя конфигурационного файла может отличаться в зависимости от операционной системы, версии сборки сервера БД и т. п.

Например, параметр может находиться в файле /etc/mysql/mariadb.conf.d/50-server.cnf (Linux Debian) или в файле /etc/my.cnf.d/mariadb-server.cnf (RHEL) в блоке параметров [mysqld].

Найдите в файле блок [mysqld] и добавьте или измените параметр lower_case_table_names:

```
[mysqld]
lower_case_table_names=1
```

Сохраните и закройте конфигурационный файл. После этого перезапустите сервер MariaDB командой:

```
sudo systemctl restart mariadb
```

или командой:

```
sudo service mysql restart
```

2.1.3. Создайте на сервере БД пользователя, от имени которого будет работать сервер СКУД. Предоставьте ему полные права на базы TC-DB-MAIN, TC-DB-LOG, AUTH, EVENTS, NOTIFICATION, VISITREQUEST, SYNC. Обратите внимание на то, что имена баз TC-DB-MAIN и TC-DB-LOG в запросе необходимо заключить в обратные кавычки.

Например, так создаётся пользователь sigur с паролем my_password:

```
mysql
MariaDB [(none)]> CREATE USER 'sigur'@'%' IDENTIFIED BY 'my_password';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON `TC-DB-MAIN`.* TO 'sigur'@'%';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON `TC-DB-LOG`.* TO 'sigur'@'%';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON AUTH.* TO 'sigur'@'%';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON EVENTS.* TO 'sigur'@'%';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON NOTIFICATION.* TO 'sigur'@'%';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON VISITREQUEST.* TO 'sigur'@'%';
MariaDB [(none)]> GRANT ALL PRIVILEGES ON SYNC.* TO 'sigur'@'%';
MariaDB [(none)]> FLUSH PRIVILEGES;
```

2.2. Настройки для удалённого подключения рабочих мест к БД Sigur.

Если планируется использовать удалённые рабочие места Sigur, то возможны следующие варианты настройки:

1. После установки ПО Sigur включить опцию «Перенаправлять запросы к БД СКУД через сервер СКУД» через ПО «Управление сервером» или с помощью утилиты AdminCLI.

2. Альтернативно можно разрешить подключения с других хостов в настройках сервера БД. Настройки для MariaDB описаны ниже.

- Это можно сделать, отредактировав параметр bind-address. Для этого в том же файле конфигурации сервера БД (см. пункт 2.1.2 выше) под блоком [mysqld] добавьте или измените параметр:

```
bind-address=0.0.0.0
```

- Сохраните и закройте конфигурационный файл. После этого перезапустите сервер MariaDB командой:

```
sudo systemctl restart mariadb
```

3. Установка ПО Sigur.

Актуальные версии пакетов можно найти на нашем сайте.

3.1. Установка основных пакетов.

Пакеты, обязательные к установке на сервер СКУД:

- **spnxclient** – пакет клиента.
- **spnxserver** – пакет сервера. Зависит от пакета веб-сервисов.
- **sigur-web-services** – пакет веб-сервисов. Зависит от пакетов клиента и сервера.

Опциональные пакеты:

- **spnxclient-libs** – опциональный .rpm-пакет с библиотеками клиента для работы с настольными считывателями MR100 USB, ACR1252U, 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.

Linux Debian	Скачайте и установите: 1. Пакет клиента СКУД и все его зависимости (пакет spnxclient). *sudo dpkg -i spnxclient_*all.deb* 2. Пакет сервера СКУД и все его зависимости (пакет spnxserver). *sudo dpkg -i spnxserver_*.deb* 3. Пакет веб-сервисов СКУД и все его зависимости (пакет sigur-web-services). *sudo dpkg -i sigur-web-services_*.deb* Если на этом компьютере планируется использовать настольный USB-считыватель MR100 USB или ACR1252U, то дополнительно выполните шаги из пункта 3.2.2.
RHEL	Скачайте и установите пакеты клиента, сервера и веб-сервисов. Если на этом компьютере планируется использовать настольные USB-считыватели, то установите также пакет библиотек spnxclient-libs. После этого, при необходимости, выполните шаги из пункта 3.2.2. Пример команды для установки всех компонентов: *sudo rpm -i spnxclient-1*.rpm spnxclient-libs*.rpm spnxserver*.rpm sigur-web-services*.rpm*

3.2. Установка дополнительных компонентов.

3.2.1. Если на сервере будет использоваться HASP ключ лицензии, то необходимо установить драйвер HASP (Sentinel LDK and Sentinel HASP Run-time Environment DEB Installer for Linux или Sentinel HASP/LDK RedHat and SuSE RPM Runtime Installer). 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
```

3.2.2. Если на компьютере планируется использовать настольный считыватель MR100 USB или ACR1252U, то необходимо:

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

Linux Debian	*sudo apt-get install pcscd* *sudo systemctl enable pcscd* *sudo systemctl start pcscd*
RHEL	*sudo yum install pcsc-lite* *sudo systemctl enable pcscd* *sudo systemctl start pcscd*

- Установить драйвер настольного считывателя. Скачать файлы можно с официального сайта производителя:

  - MR100 USB: Linux Debian, RHEL.
  - ACR1252U. Архив содержит драйверы для разных дистрибутивов и для разных архитектур. Установите драйвер для вашей операционной системы.

    Ниже приведены примеры команд для установки драйверов.

MR100 USB	**Linux Debian**	*sudo dpkg -i libsigurccid_1.5.2-1_amd64.deb*
	RHEL	*sudo rpm -i libsigurccid-1.5.2-1.el7.x86_64.rpm*
ACR1252U	**Linux Debian**	Пример 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*
	RHEL	Пример 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*

4. Настройка подключения к БД.

Для настройки вы можете использовать утилиту командной строки AdminCLI или программу «Управление сервером».

4.1. Настройка через AdminCLI.

- Установите тип используемой базы данных.
- Установите хост подключения к БД.
- Установите порт подключения к БД (порт MariaDB по умолчанию – 3306).
- Установите логин пользователя БД.
- Установите пароль для подключения к БД.

Пример команд:

```
spnxcli database setType mysql
spnxcli database setHost 127.0.0.1
spnxcli database setPort 3306
spnxcli database setLogin sigur
spnxcli database setPassword my_password
```

- Инициализируйте БД.

```
spnxcli database reset
```

- Выполните попытку подключения. Убедитесь, что тест завершился успешно. В противном случае проверьте реквизиты подключения к БД.

```
spnxcli database test
```

4.2. Настройка через ПО «Управление сервером».

- Запустите программу «Управление сервером» из меню окружения вашего рабочего стола или командой:

```
sudo spnxadmin
```

- Во вкладке «База данных» нажмите кнопку «Параметры».
- В открывшемся окне введите параметры подключения к серверу БД: адрес хоста, порт (порт MariaDB по умолчанию – 3306), имя пользователя БД и пароль. Сохраните настройки и закройте окно.
- На вкладке «База данных» нажмите кнопку «Сброс/Создание базы». Убедитесь, что процесс создания БД не сопровождался ошибками, а параметр «Статус сервисных БД» имеет значение OK.
- Вернитесь в окно настроек параметров подключения к серверу БД и нажмите кнопку «Тест подключения». Убедитесь, что тест завершился успешно. В противном случае проверьте реквизиты подключения к БД.

5. Запуск серверного модуля.

После настройки подключения к БД необходимо выполнить запуск серверного модуля для завершения конфигурирования системы. Для этого на вкладке «Состояние» ПО «Управление сервером» нажмите кнопку «Старт» или выполните команду:

```
spnxcli service startSphinxd
```

6. Запуск клиентского ПО.

Для запуска программы «Клиент» можно воспользоваться следующей командой:

```
spnxclient
```

7.1.4. Возможные проблемы после установки ПО на Linux Debian и RHEL

Если после установки ПО Sigur на ОС Linux Debian и RHEL не удаётся запустить серверный модуль, рекомендуется выполнить следующее:

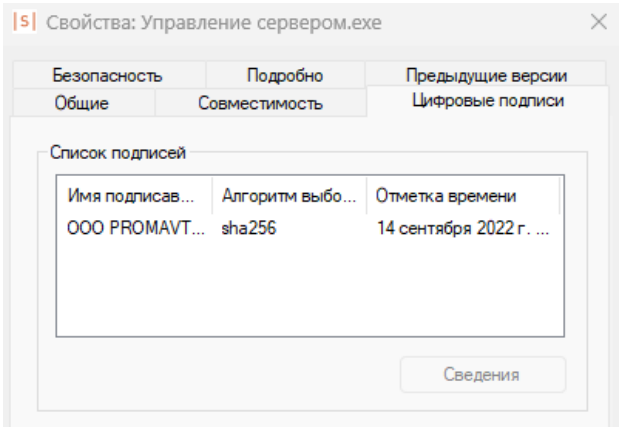
1. Проверить, что в каталоге «/var/log/sigur-ws» появились файлы generate.log и rabbit-postinstall.log. В этих файлах не должно быть ошибок.
2. Если файлы не были созданы или в них есть ошибки, то рекомендуется переустановить ПО согласно пошаговой инструкции в предыдущем разделе.
3. Если проблема сохраняется после переустановки ПО, то рекомендуется обратиться в техническую поддержку Sigur.

7.1.5. 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.

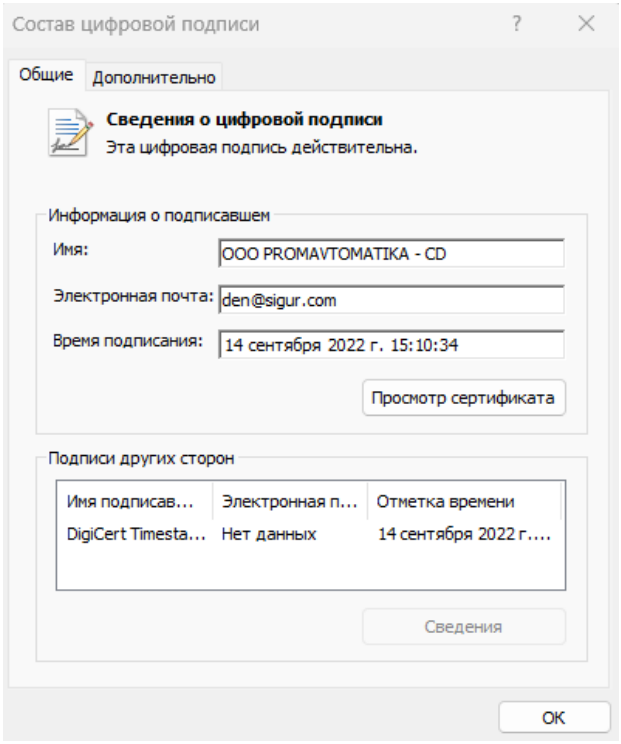
- Кликните правой кнопкой мыши по файлу инсталлятора (setup-XX.exe) или по исполняемому файлу программы («Управление сервером», «Клиент») и выберите в контекстном меню раздел «Свойства».

- 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

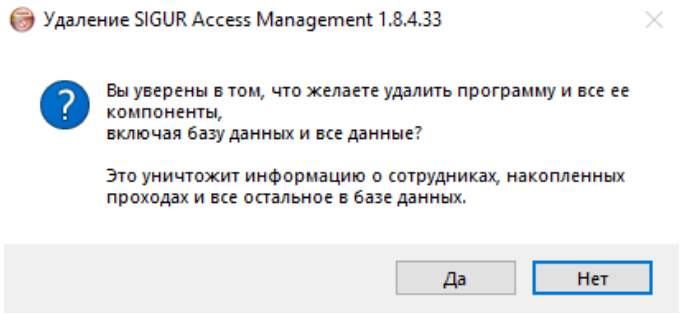
ОС Windows.

Удаление программного обеспечения Sigur производится двумя способами: ярлыком, находящимся в меню «Пуск» или с помощью «Панели управления».

Например, для Windows 10 это будут:

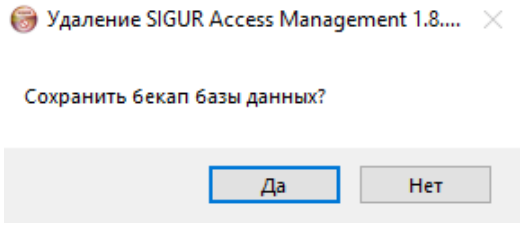
- Меню «Пуск» – «SIGUR Access Management» – «Удаление программы».
- «Панель управления» – «Установка и удаление программ» – кнопка «Заменить/удалить» в строке «SIGUR Access Management XX» (где XX – номер версии установленного ПО).

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 резервную копию (бэкап) базы данных.

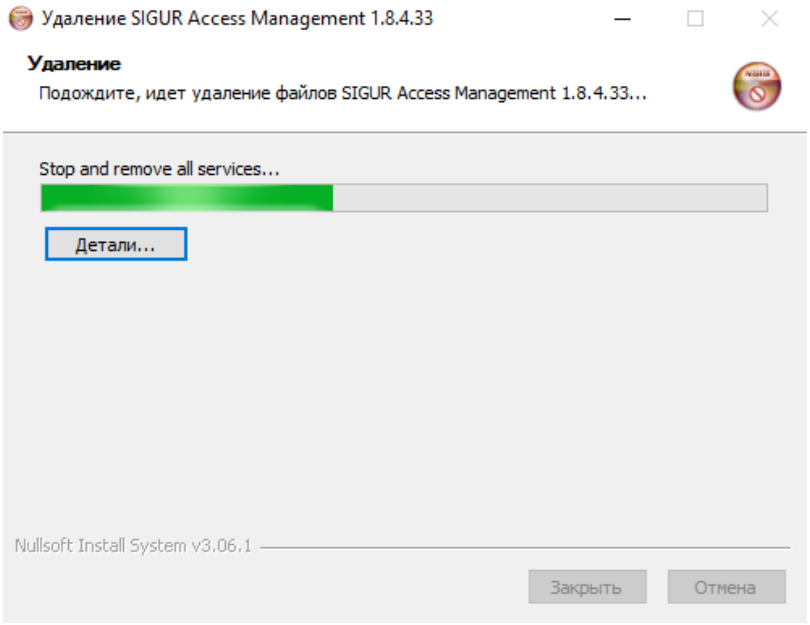


Запрос сохранения базы данных.

При нажатии кнопки «Да» в папке 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».

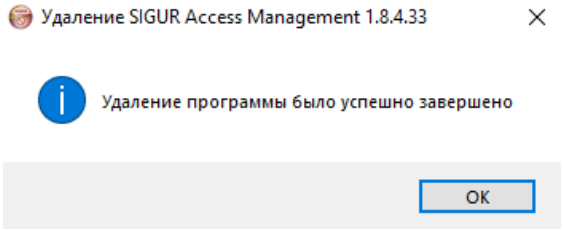
Лицензия ПО Sigur не сохраняется при создании бэкапа базы данных, её необходимо предварительно сохранить отдельно.

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



Процесс удаления программы.

После завершения процесса откроется окно с сообщением об успешном удалении программы, где нужно нажать «ОК».



Завершение удаления программы.

ОС Linux.

Пример команд для удаления ранее установленных пакетов:

Linux Debian	*sudo dpkg -r spnxclient spnxserver sigur-web-services*
RHEL	*sudo rpm -e spnxclient spnxclient-libs spnxserver sigur-web-services*

Данные команды никак не затрагивают саму базу данных, т. к. в случае сервера под управлением ОС Linux она администрируется штатными средствами СУБД.

7.4. Обновление системы Sigur

Обновление системы Sigur выполняется поверх ранее установленного программного обеспечения. Актуальные версии ПО Sigur можно скачать, перейдя по этой ссылке.

Перед обновлением рекомендуется выполнить резервное копирование данных. Процедура описана в соответствующем разделе. Также следует убедиться в наличии свободного места на диске (не менее размера базы данных), поскольку в процессе обновления часть данных может временно копироваться, из-за чего объём занимаемого дискового пространства может увеличиться до двух раз.

ОС Windows.

Для обновления сервера необходимо:

1. Закрыть все графические окна ПО Sigur.
2. Запустить файл setup-XX.exe (где XX – номер версии ПО), аналогичный тому, из которого производилась установка системы. Установщик определит необходимость и возможность обновления автоматически. Следуйте инструкциям установщика, чтобы пройти все шаги процесса обновления ПО.
3. По завершении обновления запустить ПО «Управление сервером» и нажать кнопку «Старт» на вкладке «Состояние».
4. Если после запуска системы 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:

- папке установки программы;
- ветке реестра HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\ACS Sphinx.

При использовании интеграции с системой Ewclid, дополнительно требуется предоставить доступ к:

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

ОС Linux.

Процедура обновления сервера:

1. **Остановка системы Sigur.**
   Остановите серверный модуль, нажав кнопку «Стоп» на вкладке «Состояние» ПО «Управление сервером», или выполнив команду:

   ```
   spnxcli service stopSphinxd
   ```

   Проверить статус системы можно, выполнив команду:

   ```
   spnxcli service status
   ```

   После этого необходимо закрыть все графические окна системы Sigur (если применимо).

2. **Удаление предыдущей версии Java.**
   Для работы ПО Sigur требуется Java 17. Уточнить версию Java можно командой:

   ```
   java --version
   ```

   Если версия Java отличается от 17, необходимо ее переустановить. Например, удалить Java 11 перед последующей переустановкой можно следующими командами:

Linux Debian	*sudo apt purge openjdk-11**
RHEL	*sudo yum remove java-11**

3. **Установка Java 17.**
Пример команд для установки Java 17:

Linux Debian	*sudo apt-get update* *sudo apt-get install openjdk-17-jre*
RHEL	*sudo yum update* *sudo yum install java-17-openjdk*

Проверьте итоговую версию Java. Команда должна вывести информацию о Java версии 17.

```
java --version
```

4. **Обновление ПО Sigur.**
Загрузите пакеты актуальной версии ПО и выполните команды, представленные ниже (пример).

Linux Debian	Выполнить команды последовательно: *dpkg -i spnxclient_*all.deb* *dpkg -i spnxserver_*.deb* *dpkg -i sigur-web-services_*.deb*
RHEL	Перечислить все обновляемые пакеты: *rpm -U spnxclient-1*.rpm spnxserver*.rpm spnxclient-libs*.rpm sigur-web-services*.rpm*

5. **Запуск сервера Sigur.**
По окончании обновления запустите серверный модуль, нажав кнопку «Старт» на вкладке «Состояние» ПО «Управление сервером», или выполнив команду:

```
spnxcli service startSphinxd
```

6. **Обновление версии базы данных.**
При необходимости обновите версию базы данных, нажав кнопку «Обновить» на вкладке «База данных» ПО «Управление сервером», или выполнив команду:

```
spnxcli database update
```

7. **Обновление клиентских мест.**
   Клиентские места, установленные под ОС Linux, необходимо обновить вручную. Пример команд:

Linux Debian	*dpkg -i spnxclient_*all.deb*
RHEL	Перечислить все обновляемые пакеты: *rpm -U spnxclient-1*.rpm spnxclient-libs*.rpm*

7.5. Особенности обновления на версии ПО 1.8.x.x

Условия для успешной миграции системного оператора при обновлении ПО.

При обновлении ПО на версию с ролевой моделью (1.8.x.x и выше) необходимо выполнить следующие действия:

1. Убедиться в наличии оператора с логином Administrator.
2. В случае отсутствия оператора с логином Administrator необходимо:

   - создать нового сотрудника или использовать учётную карточку существующего;
   - назначить его оператором с логином Administrator.

При обновлении ПО оператору с логином Administrator:

- назначается роль по умолчанию «Глобальный администратор»;
- снимаются наложенные ограничения (при их наличии);
- пароль оператора остаётся прежним.

После обновления будет невозможно удалить или отредактировать права оператора Administrator — он будет являться частью системы. Однако редактирование его учётной карточки (параметров доступа и других данных) останется возможным.

Если оператор с логином Administrator отсутствовал на момент обновления ПО, то для его восстановления и снятия ограничений необходимо обратиться в техническую поддержку Sigur.

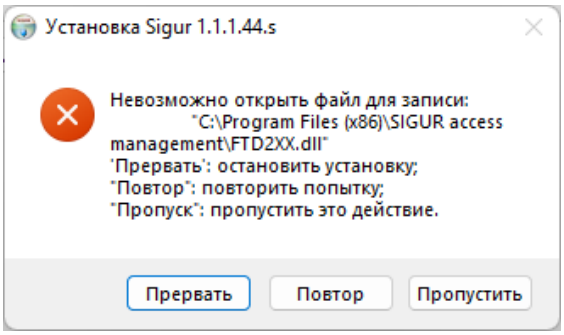
Переход на 64-разрядную архитектуру (Windows).

64-разрядная версия ПО Sigur для Windows не имеет ограничений на объём используемой сервером оперативной памяти. Это позволяет серверу СКУД обрабатывать существенно больше видеокамер и эффективнее работать с большими объёмами данных (например, при использовании интеграций с внешними системами).

Для перехода на 64-разрядную версию требуется полная переустановка программного обеспечения с последующим восстановлением из резервной копии. При необходимости возможен возврат на 32-разрядную версию тем же способом. Подробную информацию о создании и восстановлении резервной копии базы данных Sigur см. в соответствующих разделах руководства.

7.6. Возможные сообщения об ошибках при обновлении ПО

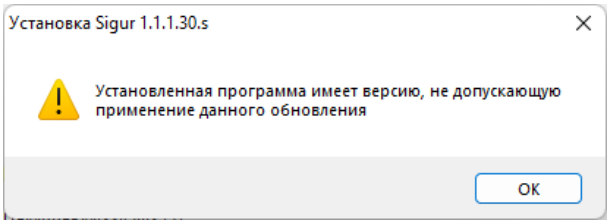
- После запуска установочного файла появляется сообщение «Невозможно открыть файл для записи: "C:\Program Files (x86)\SIGUR access managment\FTD2XX.dll"»:



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.

7.7. 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 папку 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».

7.8. 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.

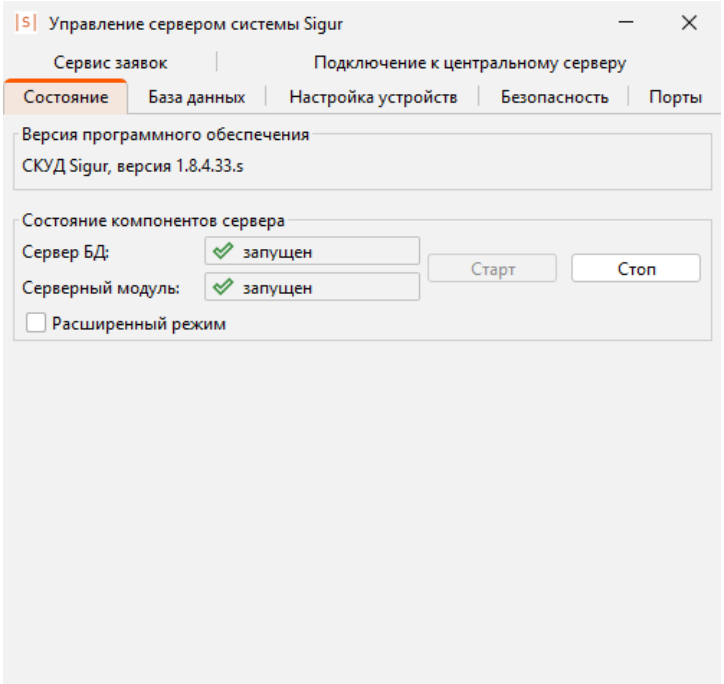
8.1. Запуск программы

Запуск программы осуществляется с помощью ярлыка «Управление сервером», расположенного в меню «Пуск» – «Программы» – «SIGUR Access Management».

8.2. Главное окно программы

Главное окно программы предоставляет пользователю все средства для управления сервером 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.

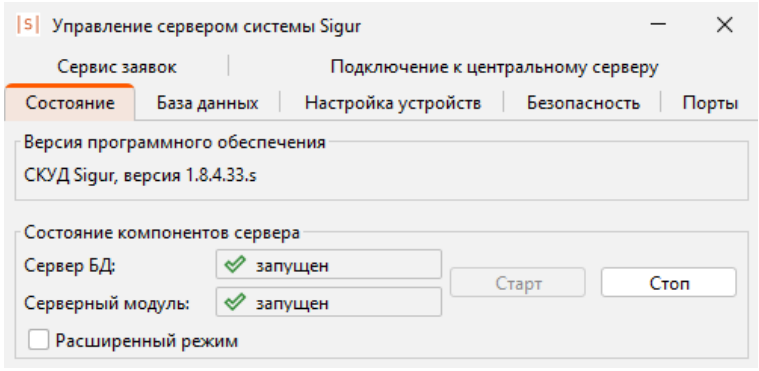
Функции управления сервером Sigur распределены по вкладкам: «Состояние», «База данных», «Настройка устройств», «Безопасность», «Порты», «Сервис заявок», «Подключение к центральному серверу».

Настройка подключения к центральному серверу приведена в «Руководстве по настройке и использованию ПО Sigur Центральный сервер», настройка сервиса заявок – в «Руководстве пользователя ПО Sigur». Описание настроек остальных вкладок приведено в соответствующих разделах ниже.

9. Управление компонентами сервера

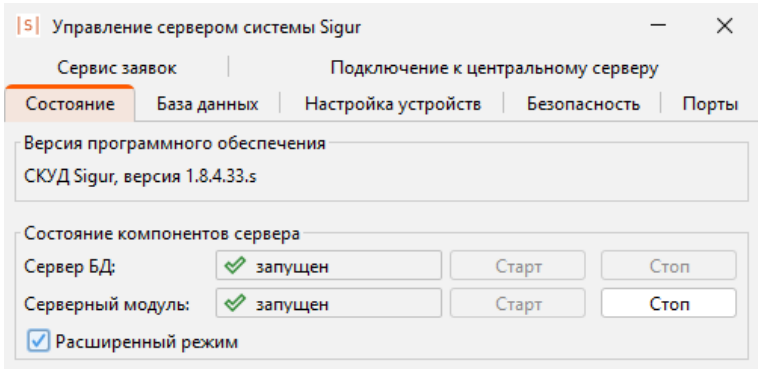
На вкладке «Состояние» ПО «Управление сервером» можно запускать, останавливать компоненты сервера и наблюдать за их состоянием. В верхнем окне вкладки отображается текущая версия программного обеспечения.

Обычный режим управления компонентами сервера:



Обычный режим управления компонентами сервера.

Расширенный режим управления компонентами сервера:



Расширенный режим управления компонентами сервера.

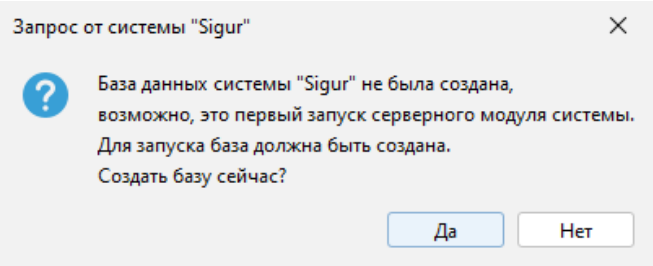
Для переключения режима управления служит функция «Расширенный режим». При выключенном расширенном режиме можно запускать и останавливать сразу оба компонента, при включённом – раздельно.

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.

При нажатии кнопки «Да» будет создана исходная база данных. База создаётся один раз, и последующие запуски сервера БД 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».

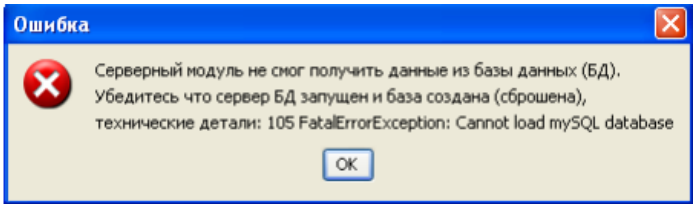
Остановка сервера БД осуществляется кнопкой «Стоп» в строке «Сервер БД».

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 система запускает ряд веб-сервисов. Поэтому время запуска сервера Sigur может достигать 2 минут.

При запуске серверного модуля с повреждённой базой данных программа выдаст следующее сообщение об ошибке:

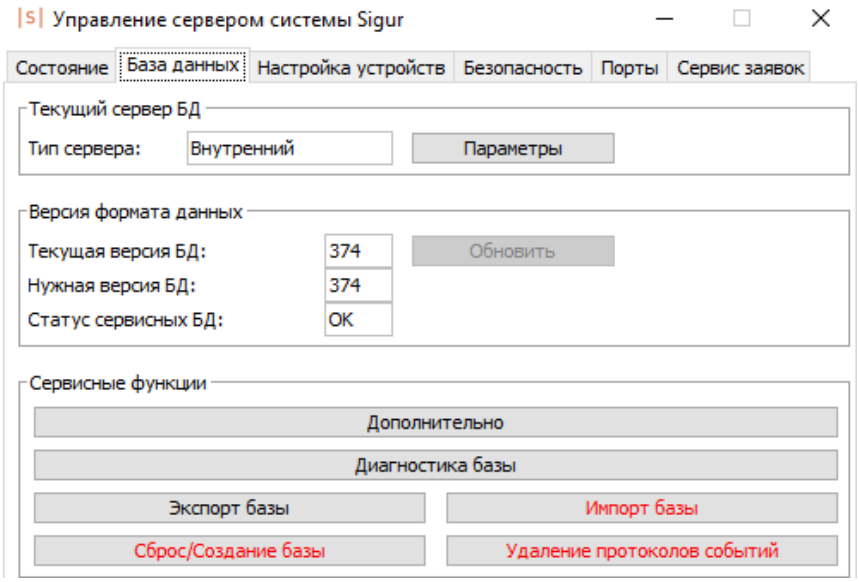


Сообщение при запуске серверного модуля с повреждённой базой данных.

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

10. Управление базой данных

Вкладка «База данных» ПО «Управление сервером» предназначена для всех операций, возможных с базой данных Sigur.



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

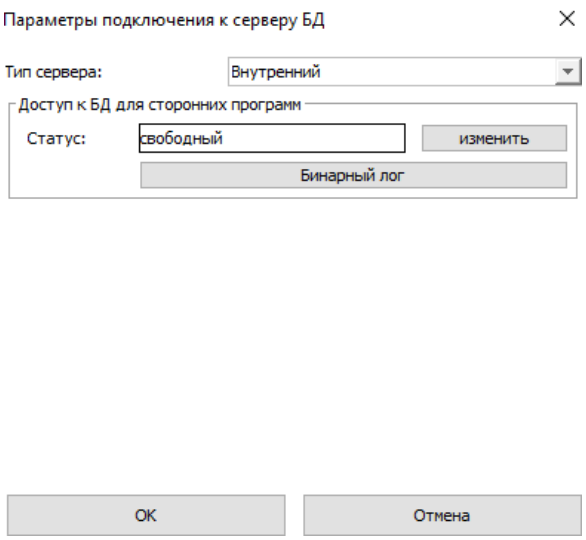
База данных используется системой для хранения информации об объектах доступа, режимах допуска, о событиях системы и т. д.

10.1. Тип сервера БД

По умолчанию на ОС Windows системой Sigur используется только внутренняя БД MariaDB. На ОС Linux возможно использовать внешнюю БД MariaDB или PostgreSQL. Для настройки подключения к серверу базы данных необходимо нажать на кнопку «Параметры» в блоке «Текущий сервер БД».

На ОС Windows пользователь может:

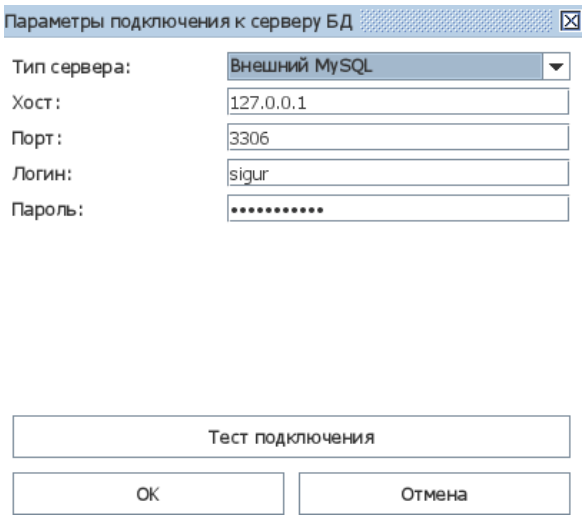
- Изменить пароль к внутренней БД. Подробнее – в соответствующем разделе.
- Включить запись бинарного лога БД для работы некоторых интеграционных сервисов. Инструкции по настройке бинарного лога содержатся в отдельных руководствах на интеграции с внешними системами.



Окно «Параметры подключения к серверу БД» на ОС Windows.

На ОС Linux возможно:

- Выбрать тип сервера – «Внешний MySQL» или «Внешний PostgreSQL».
- Заполнить реквизиты подключения к БД: хост, порт, имена БД сервера и веб-сервисов, а также имена схем этих БД (при использовании PostgreSQL), логин и пароль пользователя БД.
- Протестировать подключение к БД с помощью соответствующей кнопки.



Окно «Параметры подключения к серверу БД» на ОС Ubuntu.

10.2. Использование PostgreSQL в качестве сервера базы данных

При развёртывании серверной части Sigur на ОС Linux пользователь может выбрать тип сервера внешней базы данных – MariaDB или PostgreSQL (в том числе Postgres Pro).

База данных PostgreSQL предназначена исключительно для опытных пользователей, которые осознанно выбирают это программное обеспечение и обладают необходимыми навыками для его самостоятельного администрирования. В противном случае рекомендуется использовать в качестве БД MariaDB, для которой предоставляется полная поддержка.

Обратите внимание, что настройка и дальнейшее сопровождение БД PostgreSQL осуществляется пользователем самостоятельно. Необходимо учитывать следующие особенности:

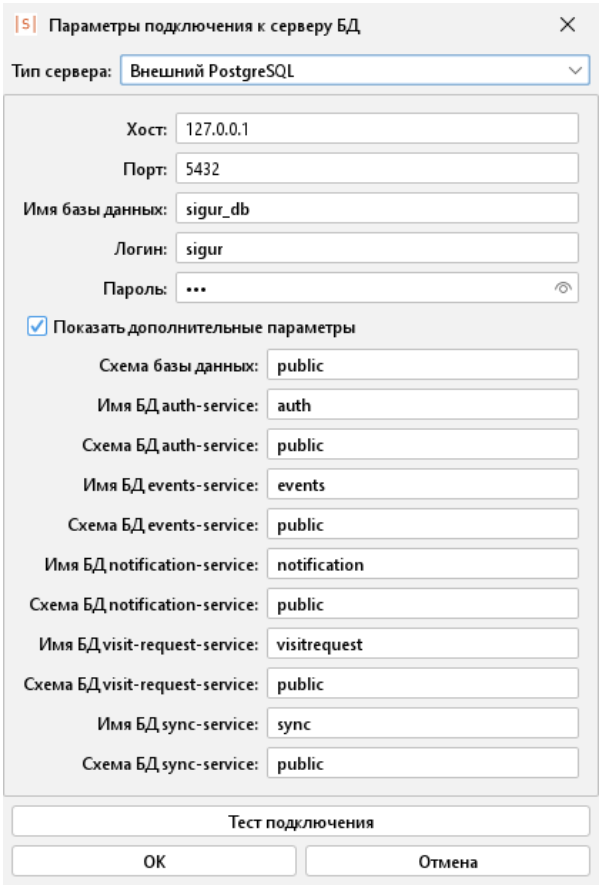
- В случае использования PostgreSQL система Sigur ожидает подключения к заранее созданной базе данных сервера СКУД. Необходимо создать чистую базу данных для её успешной инициализации. БД веб-сервисов будут созданы автоматически при инициализации БД сервера.
- Все таблицы БД Sigur по умолчанию создаются в схеме public. При необходимости имена схем можно изменить во время первичной настройки системы через ПО «Управление сервером» или утилиту AdminCLI. Для успешного запуска и дальнейшей работы системы пользователь БД, от имени которого Sigur подключается к базе, должен иметь права на указанные схемы.
- При создании бэкапов необходимо резервировать БД сервера, ранее созданную пользователем, а также БД веб-сервисов: auth, events, notification, visitrequest, sync.
- Резервная копия БД, созданная на MariaDB, не может быть загружена в PostgreSQL, и наоборот. Миграция данных между этими СУБД также невозможна.

10.3. Настройка имён БД и схем сервера и веб-сервисов (PostgreSQL)

При использовании PostgreSQL в качестве внешней БД Sigur в ходе первичной настройки системы можно задать:

- имена БД веб-сервисов СКУД;
- имена схем БД сервера и веб-сервисов.

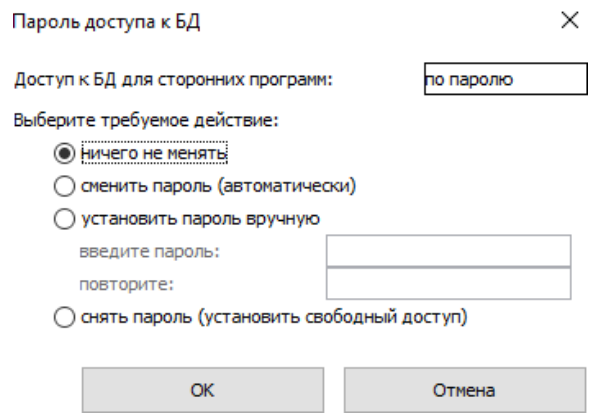
Настройка выполняется через ПО «Управление сервером» или утилиту AdminCLI. В ПО «Управление сервером» перейдите на вкладку «База данных» и нажмите кнопку «Параметры». В открывшемся окне включите опцию «Показать дополнительные параметры» и выполните необходимые настройки. Затем сохраните изменения и выполните инициализацию БД.



Настройка параметров подключения к серверу БД.

10.4. Установка пароля на доступ к базе данных на ОС Windows

Для изменения доступа сторонних программ к внутренней БД на ОС Windows необходимо нажать кнопку «Параметры» на вкладке «База данных», а далее – кнопку «Изменить». Откроется окно «Пароль доступа к БД».

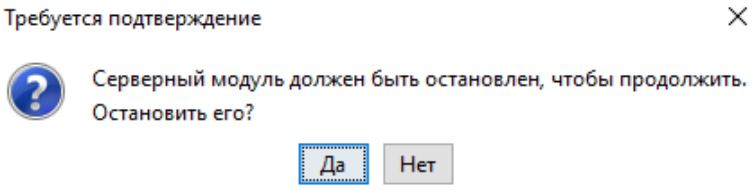


Окно «Пароль доступа к БД».

В данном окне доступны 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».

10.5. Версия формата данных

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

Панель «Версия формата данных».

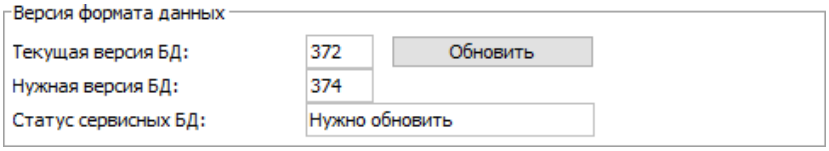
Версия БД – это характеристика базы данных, используемой программой. По мере усовершенствования системы, введения в неё новых функций и выхода новых версий ПО, может меняться формат хранения данных и, соответственно, меняется версия БД.

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.

Дополнительно в окне отображается текущий статус БД веб-сервисов системы.

10.6. 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» и меняется статус БД веб-сервисов.

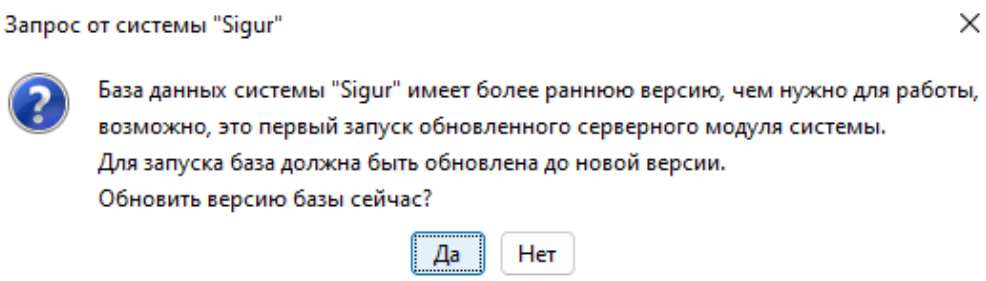


Пример отличия версий БД.

Для обновления версии баз данных 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.

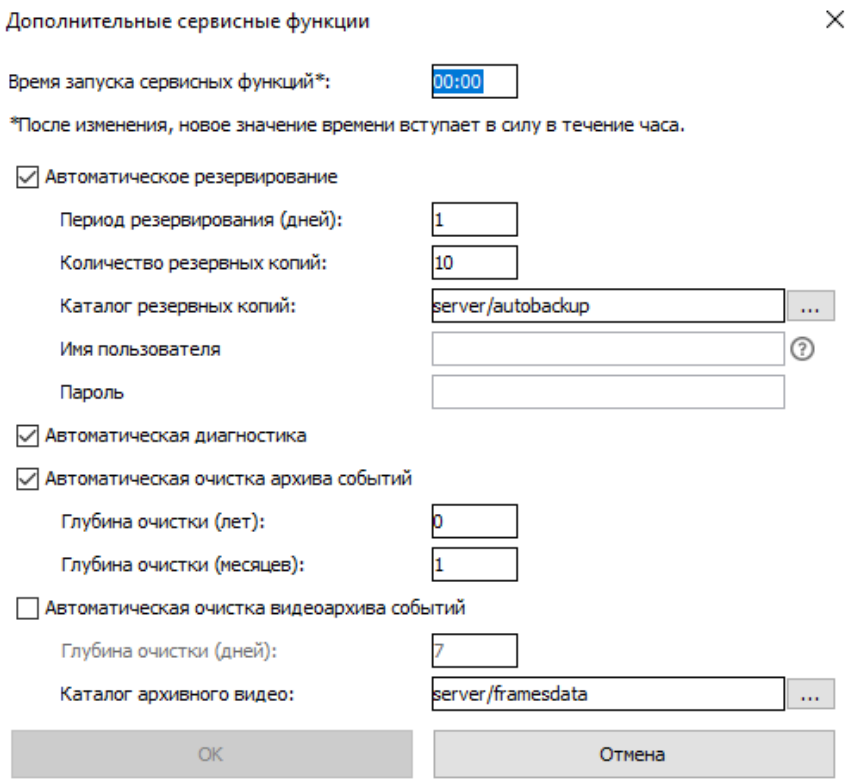


Сообщение при запуске сервера БД после обновления серверного ПО.

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

10.7. Дополнительные настройки сервера

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



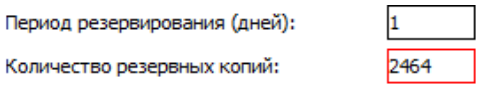
Дополнительные функции сервера.

10.8. Автоматическое резервирование (сохранение) базы данных

Доступно только на ОС Windows. 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 – 0 часов 0 минут).
4. Ввести количество последних резервных копий (от 1 до 999), которое будет хранить программа.
5. Изменить, при необходимости, папку 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 меняет цвет на красный. Пример окна, где первое значение введено корректно, а второе – нет:



Пример ввода некорректного значения.

По умолчанию резервные копии БД сохраняются в папку установленной программы:

- «C:\Program Files (x86)\SIGUR access management\server\autobackup\» (для 32-разрядной версии);
- «C:\Program Files\SIGUR access management\server\autobackup\» (для 64-разрядной версии).

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

Старые копии автоматически удаляются.

10.9. Автоматическая диагностика базы данных

Доступно только на ОС Windows. 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 – 0 часов 0 минут).

10.10. Автоматическая очистка архива событий

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

10.11. Автоматическая очистка видеоархива событий

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

По умолчанию видеоархив сохраняется:

- Windows: в папку установленной программы. Путь по умолчанию:
  - C:\Program Files (x86)\SIGUR access management\server\framesdata\ (для 32-разрядной версии);
  - C:\Program Files\SIGUR access management\server\framesdata\ (для 64-разрядной версии).
- Linux: в каталог /var/lib/sphinxacs/framesdata.

При использовании пользовательской директории на ОС Linux необходимо предоставить пользователю *sphinx* права на запись в эту директорию.

Процесс *sphinxd* запускается от имени данного пользователя, поэтому, если директория создана другим пользователем и у *sphinx* отсутствуют права на запись, создание файлов в ней будет невозможно.

10.12. Сохранение (экспорт) базы данных

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

Лицензия ПО Sigur не сохраняется при создании бэкапа базы данных – её необходимо сохранить отдельно.

ОС Windows.

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».

ОС Linux.

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

В частности, для создания резервных копий БД MariaDB можно использовать следующую команду:

```
mysqldump -u <user> -P 3306 -p <userpass> -B TC-DB-MAIN TC-DB-LOG AUTH EVENTS NOTIFICATION VISITREQUEST SYNC > backup.sql
```

Здесь:

- <user> – имя пользователя БД.
- <userpass> – пароль указанного пользователя БД.
- TC-DB-MAIN, TC-DB-LOG, AUTH, EVENTS, NOTIFICATION, VISITREQUEST, SYNC – наименования используемых БД.

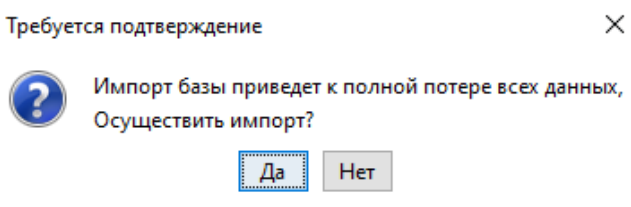
10.13. Восстановление (импорт) базы данных

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

ОС Windows.

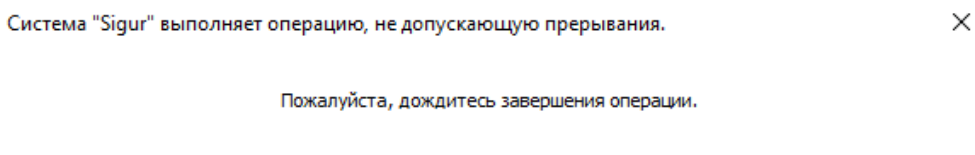
Импорт базы данных может потребоваться при переносе системы на другой компьютер или серьёзном сбое, вызвавшем повреждение структуры БД, которое неустранимо с помощью операции «Диагностика базы данных».

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».

ОС Linux.

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

Бэкап БД MariaDB не может быть загружен на PostgreSQL, и наоборот. Также миграция данных между этими СУБД невозможна.

В частности, для загрузки в систему готового бэкапа БД MariaDB можно воспользоваться командой:

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

Здесь:

- <user> – имя пользователя БД.
- <userpass> – пароль указанного пользователя БД.
- backup.sql – наименование импортируемого файла с бэкапом БД.

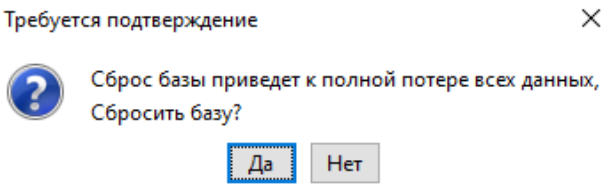
Если файл бэкапа изначально был сформирован на сервере под управлением ОС Windows, необходимо предварительно отключить чувствительность к регистру в настройках сервера БД MariaDB (см. раздел «Установка системы Sigur»).

10.14. Сброс/создание базы данных

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

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

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

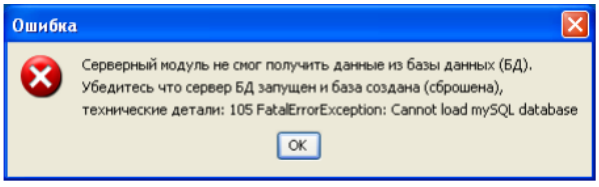


Запрос подтверждения сброса базы данных.

10.15. Диагностика (ремонт) базы данных

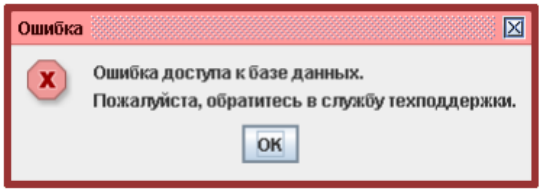
Эта функция позволяет устранять некоторые повреждения данных, возникшие, например, в результате аварийного завершения работы системы (зависание, выключение питания компьютера и т. д.).

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». Недоступно в случае использования БД PostgreSQL на ОС Linux.

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.

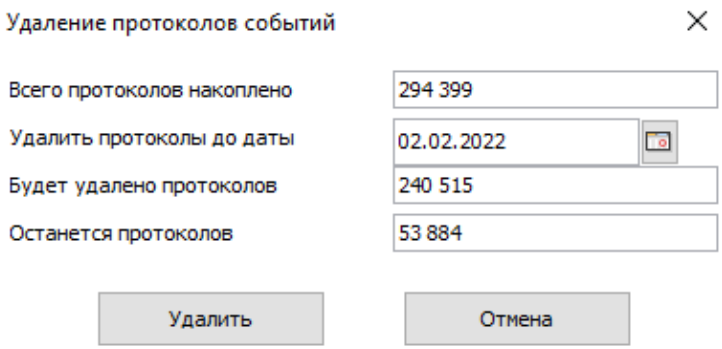
Если после этого сообщения об ошибках продолжают появляться – обратитесь в службу технической поддержки Sigur.

10.16. Удаление протоколов событий

Эта функция позволяет удалять протоколы событий 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 будут удалены протоколы. Протоколы за указанную дату сохраняются. По умолчанию в данном поле установлена дата на год ранее текущей.
- «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 необходимо удалить протоколы событий, и нажмите «Удалить», затем подтвердите операцию.

11. Настройка IP-устройств

Настройка IP-параметров устройств может выполняться с помощью ПО «Управление сервером». На вкладке «Настройка устройств» доступны настройка IP-параметров контроллеров Sigur и просмотр списка устройств, обнаруженных в текущей сети.

Для большинства моделей контроллеров также доступна настройка IP-параметров с помощью утилиты «DCT». Утилита предназначена для быстрой настройки параметров контроллеров и, в отличие от ПО «Управление сервером», позволяет выполнять настройку устройств, находящихся в другой сети. Подробное описание работы утилиты и список поддерживаемых моделей контроллеров приведены в отдельном документе.

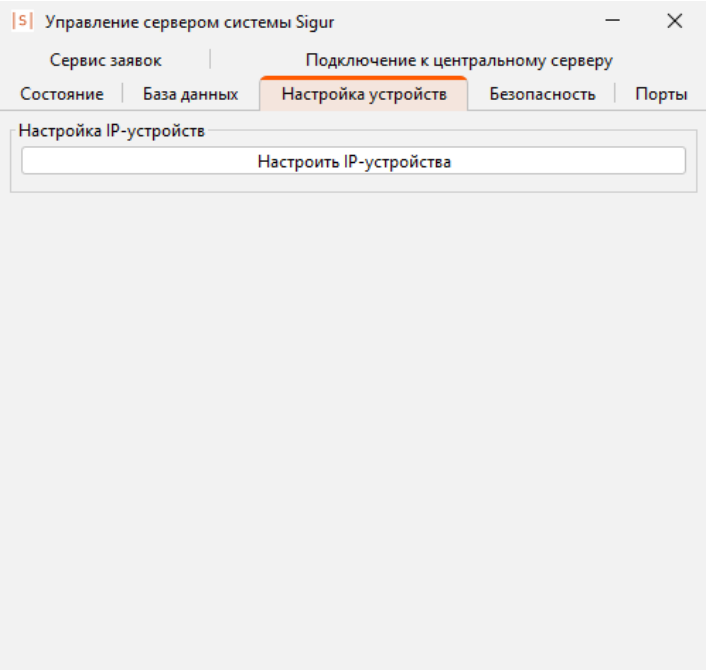
Далее приведено описание процесса настройки IP-параметров контроллеров с помощью ПО «Управление сервером».

11.1. Добавление и настройка IP-устройств

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 техподдержку Sigur.

Предварительно отключите 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 Sigur или изменения IP-параметров уже добавленного устройства запустите программу «Управление сервером», расположенную в меню «Пуск» – «Программы» – «SIGUR Access Management». Выберите вкладку «Настройка устройств» и нажмите кнопку «Настроить IP-устройства».

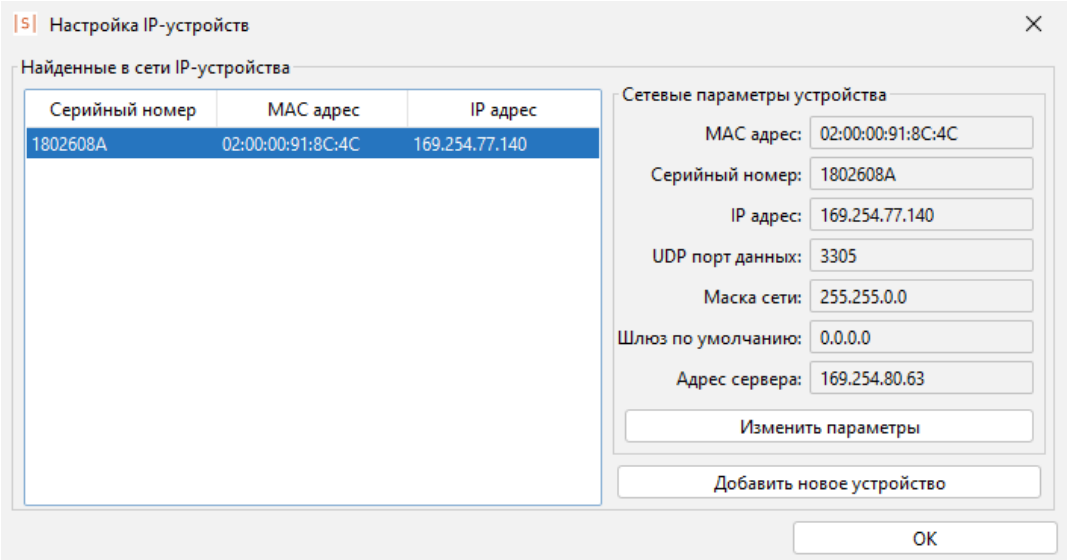


Вкладка «Настройка устройств».

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 и не требует наличия лицензий.

Открывшееся окно содержит список устройств с уже настроенными IP-параметрами (до которых доходят широковещательные запросы по порту UDP 3303 в этом сегменте IP-сети). Список можно отсортировать по возрастанию или убыванию, нажав на заголовок любого столбца. В столбце «Серийный номер» отображаются серийные номера контроллеров E510, E2, E4 и более новых с версией микропрограммы 0.21.0 и выше.

При выборе в списке конкретного устройства в правой части окна отображаются его текущие IP-параметры, а также становится доступна кнопка «Изменить параметры». Если для подключения к серверу используется FQDN, в панели будет отображаться IP-адрес сервера. При необходимости значение любого параметра можно выделить и скопировать (Ctrl+C или правой кнопкой мыши).



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

Контроллеры Sigur нового поколения (E510, E2, E4 и др.) 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».

Далее возможны два варианта:

1. В списке «Найденные в сети IP-устройства» уже присутствует строка с MAC-адресом вашего контроллера. В этом случае выделите её и нажмите кнопку «Изменить параметры». При необходимости введите пароль доступа к настройкам (по умолчанию – sigur), затем нажмите «OK».
2. Список «Найденные в сети IP-устройства» пуст. При использовании контроллеров E510, E2, E4 и более новых проверьте настройки сети, сетевых фильтров и антивирусных программ. При использовании контроллеров предыдущих поколений нажмите кнопку «Добавить новое устройство» и следуйте инструкциям, описанным далее.

11.1.1. Добавление нового устройства

Данная инструкция не актуальна для контроллеров моделей E2, E4, E510 и более новых. При настройке данных моделей необходимо сразу переходить к разделу «Изменение IP-параметров 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 будет присвоен 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.

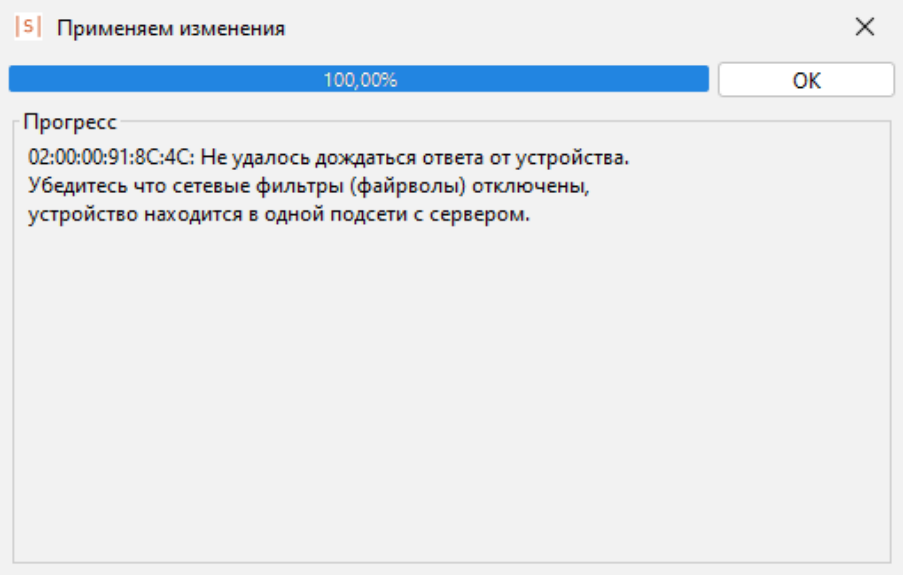
- Пароль. Значение пароля по умолчанию уже введено в поле. При необходимости изменения пароля выделите пункт «Изменить пароль», после чего станут доступны поля для ввода и подтверждения нового пароля.

  Пароль может содержать только латинские буквы, цифры, специальные символы и пробелы. Допустимая длина – от 1 до 15 символов включительно. Чтобы проверить введённый пароль, нажмите на иконку глаза.

При явных ошибках ввода рамка поля подсвечивается красным, кнопка «ОК» становится неактивной. После ввода всех параметров нажмите «ОК».

При успешном завершении процесса в списке устройств появится строка с

MAC и IP-адресами настроенного контроллера. Если же программа выдаст сообщение об ошибке – значит, по какой-либо причине серверу не удалось установить связь с контроллером.



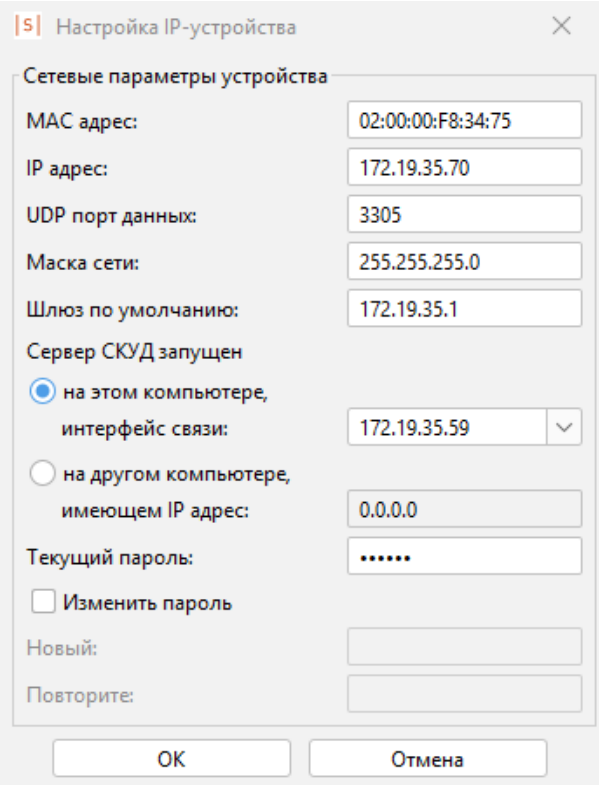
Ошибка при попытке настройки IP-параметров.

11.1.2. Изменение IP-параметров устройства

Для изменения IP-параметров выберите в списке нужный контроллер и нажмите кнопку «Изменить параметры». При необходимости введите пароль доступа к настройкам (по умолчанию – sigur), затем нажмите «ОК».

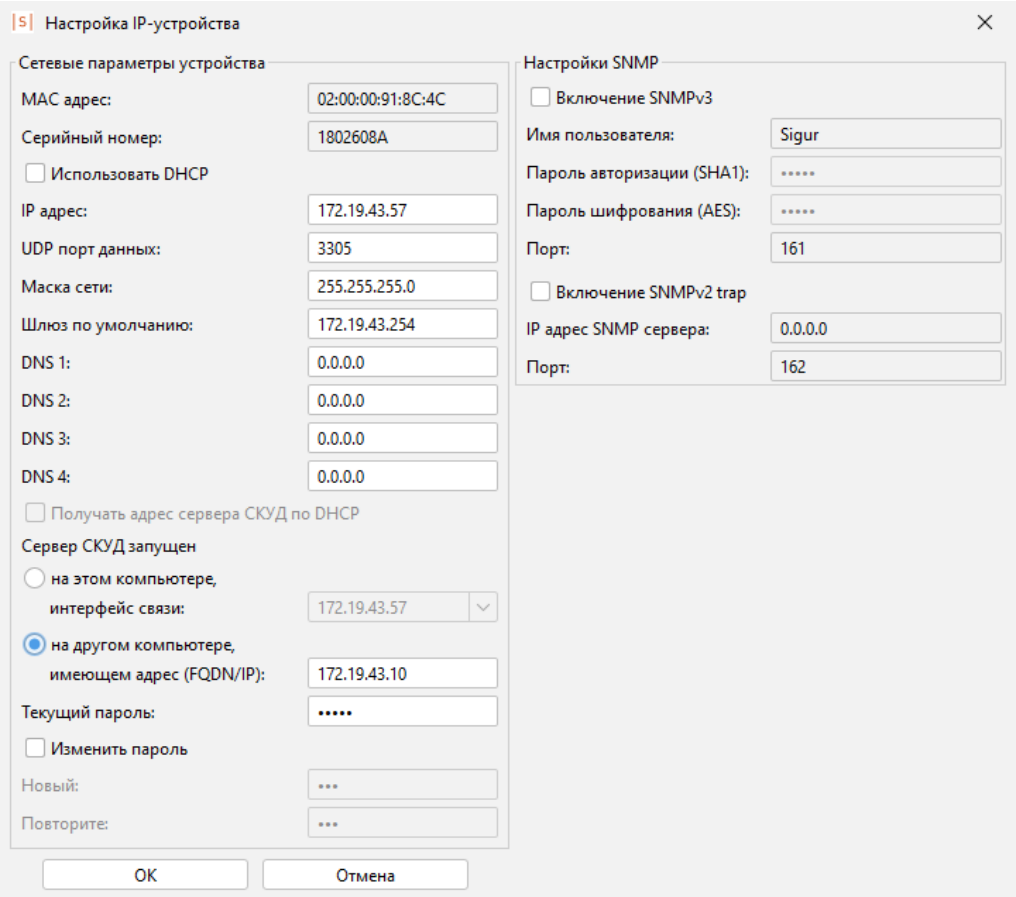
Окно «Настройка IP-устройства» имеет разный вид в зависимости от модели контроллера и поддерживаемых функций:

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



Окно «Настройка IP-устройства», вариант 1.

- Для моделей E510, E2, E4, E310 и более новых отображается расширенный вариант окна – см. рисунок «Настройка IP-устройства, вариант 2». Область «Сетевые параметры устройства» предназначена для конфигурирования IP-параметров контроллера. Набор доступных для настройки полей зависит от версии микропрограммы контроллера.



Окно «Настройка IP-устройства», вариант 2.

При открытии окна редактирования параметров поле «Текущий пароль» заполняется автоматически. Если поле не заполнено, используйте значение по умолчанию из документации на устройство. Чтобы проверить введённый пароль, нажмите на иконку глаза.

При необходимости пароль доступа к настройкам контроллера можно изменить. Для этого введите текущий пароль, затем укажите новый пароль дважды и сохраните изменения. Новый пароль может содержать только латинские буквы, цифры, специальные символы и пробелы. Допустимая длина – от 1 до 15 символов включительно.

Для всех найденных в сети устройств возможно групповое изменение некоторых IP-параметров. Для этого выделите нужные устройства, нажмите кнопку «Изменить параметры» и введите пароль доступа к настройкам. В открывшемся окне можно переопределить маску сети, шлюз по умолчанию, IP-адрес сервера СКУД и пароль.

Использование FQDN сервера СКУД и DNS.

Контроллер поддерживает возможность использования доменного имени (FQDN) сервера СКУД вместо IP-адреса. Это позволяет устанавливать соединение с сервером СКУД по доменному имени в условиях динамической

сетевой инфраструктуры.

Доступны два варианта задания FQDN:

- Статический адрес. Выберите опцию «Сервер СКУД запущен на другом компьютере, имеющем адрес (FQDN/IP)» и укажите FQDN сервера СКУД.
- Получение по DHCP. Включите опцию «Получать адрес сервера СКУД по DHCP». В этом случае контроллер будет ожидать адрес от DHCP-сервера. Потребуется настройка на стороне DHCP-сервера (см. соответствующий раздел).

Для работы с FQDN контроллеру требуется доступ к DNS-серверу.Способ настройки зависит от того, как контроллер получает свои сетевые параметры:

- Если контроллер использует статические сетевые параметры – укажите адреса DNS-серверов в соответствующих полях (до 4 адресов).
- Если контроллер получает сетевые параметры по DHCP – поля для ввода неактивны, адреса DNS-серверов должны быть получены по DHCP.
- Если требуется получать сетевые параметры контроллера по DHCP, но при этом использовать статические адреса DNS-серверов, воспользуйтесь «Утилитой настройки параметров контроллеров Sigur». Настройка данного сценария недоступна в текущей версии ПО.

Контроллер проверяет актуальность IP-адреса сервера СКУД с интервалом, определяемым значением TTL из DNS-ответа. При потере связи с сервером контроллер запрашивает у DNS-сервера IP-адрес, соответствующий FQDN сервера СКУД, с экспоненциальной задержкой между попытками. В случае недоступности одного DNS-сервера контроллер обращается к следующему.

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 активировать получение адреса сервера СКУД от DHCP-сервера (для корректной работы функции требуется провести дополнительные настройки на стороне DHCP-сервера). Подробнее – см. соответствующий раздел.

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. Подробнее – см. соответствующий раздел.

Актуальную версию файла mib-библиотеки, а также готовый шаблон конфигурации для загрузки в ПО Zabbix можно найти на странице сайта в разделе «Прочее».

11.1.3. Получение IP-параметров по DHCP

> ⚠ Чтобы уточнить, поддерживает ли конкретная модель контроллера получение IP-параметров по DHCP, обратитесь к руководству по эксплуатации контроллера.

Контроллеры Sigur могут получать по DHCP следующий набор параметров:

- IP-адрес;
- маска сети;
- шлюз;
- IP-адреса DNS-серверов (до 4 адресов);
- IP-адрес или FQDN (доменное имя) сервера СКУД.

На стороне контроллера должны быть включены опции «Использовать DHCP» и/или «Получать адрес сервера СКУД по DHCP». Контроллер поставляется с включёнными опциями, а также они активируются автоматически после сброса IP-параметров или аппаратного сброса. Если ранее контроллеру были заданы статические IP-параметры, переключить его на работу по DHCP можно 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. В открывшемся окне введите пароль доступа к настройкам (по умолчанию – sigur).
5. Включите опции «Использовать DHCP» и, если необходимо, «Получать адрес сервера СКУД по DHCP». Поля для ручного ввода IP-параметров при

этом станут неактивны.
6. Нажмите «ОК».

Для назначения IP-адреса, маски подсети, шлюза и адресов DNS дополнительные настройки на стороне DHCP-сервера в общем случае не требуются.

Если требуется передавать контроллерам 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, то в ответе должно передаваться 4 байта IP-адреса сервера СКУД в опции 43, подопции 1. Если необходимо передать FQDN сервера, то используйте опцию 43, подопцию 2.

Например, если необходимо сообщить контроллеру IP-адрес сервера 172.19.40.10, то значение опции 43 должно быть следующим (в HEX) – 0104AC13280A, где:

- 01 – suboption;
- 04 – длина передаваемой полезной информации;
- AC13280A – IP-адрес сервера СКУД: (HEX) AC 13 28 0A = (DEC) 172 19 40 10.

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.
6	Адреса DNS-серверов	Список IP-адресов DNS-серверов (до 4 адресов).
12	Имя хоста	Имя хоста контроллера. По умолчанию соответствует Sigur-XXX-YYY, где XXX – модель контроллера, YYY – серийный номер. Значение может быть изменено через «Утилиту настройки параметров контроллеров Sigur». После сброса сетевых параметров контроллера или аппаратного сброса возвращается к значению по умолчанию.

Номер опции	Значение опции	Примечание
43	Специфичная информация производителя	Используется для указания адреса сервера СКУД. Поддерживаются две подопции: • suboption 1 – IP-адрес сервера СКУД; • suboption 2 – FQDN сервера СКУД.
60	Идентификатор производителя	По умолчанию соответствует Sigur PACS Unit. Значение может быть изменено через «Утилиту настройки параметров контроллеров Sigur». После сброса сетевых параметров контроллера или аппаратного сброса возвращается к значению по умолчанию.
77	Информация о пользовательском классе	По умолчанию соответствует Sigur-XXX, где XXX – модель контроллера. Значение может быть изменено через «Утилиту настройки параметров контроллеров Sigur». После сброса сетевых параметров контроллера или аппаратного сброса возвращается к значению по умолчанию.

11.2. Аутентификация контроллеров по EAP-TLS (IEEE 802.1X)

Чтобы уточнить, поддерживает ли конкретная модель контроллера аутентификацию по EAP-TLS, обратитесь к руководству по эксплуатации контроллера.

В Sigur реализована поддержка аутентификации контроллеров в защищённом сегменте сети с использованием метода EAP-TLS в рамках стандарта IEEE 802.1X. Этот метод используется для защиты сети от несанкционированного доступа.

Для аутентификации используются те же сертификаты, что и для защищённого взаимодействия контроллера с сервером СКУД по протоколу DTLS, добавленные в пользовательский профиль шифрования. Дополнительных действий со стороны пользователя не требуется.

При использовании IEEE 802.1X контроллер проходит аутентификацию на выделенном сервере (например, RADIUS) через сетевое устройство (например, коммутатор). Для этого используется протокол EAP-TLS, в рамках которого по защищённому соединению происходит взаимная проверка сертификатов.

После успешной аутентификации коммутатор открывает доступ к сети и контроллер устанавливает с сервером СКУД защищённое соединение.

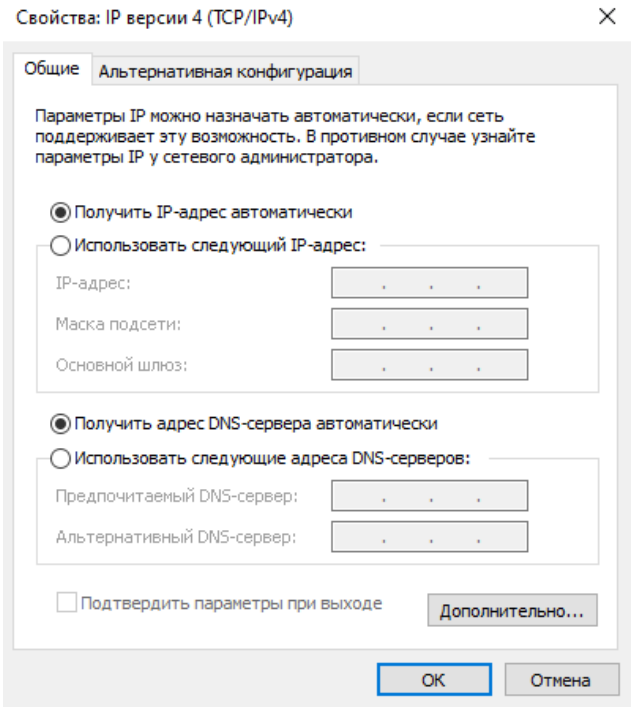
Первичная загрузка профиля шифрования на контроллер может быть выполнена в сетевом сегменте без аутентификации по 802.1X. Подробную информацию о настройке DTLS см. в разделе «Шифрование трафика между сервером и контроллерами по DTLS».

11.3. Возможные причины неудачной настройки IP-параметров

- 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.

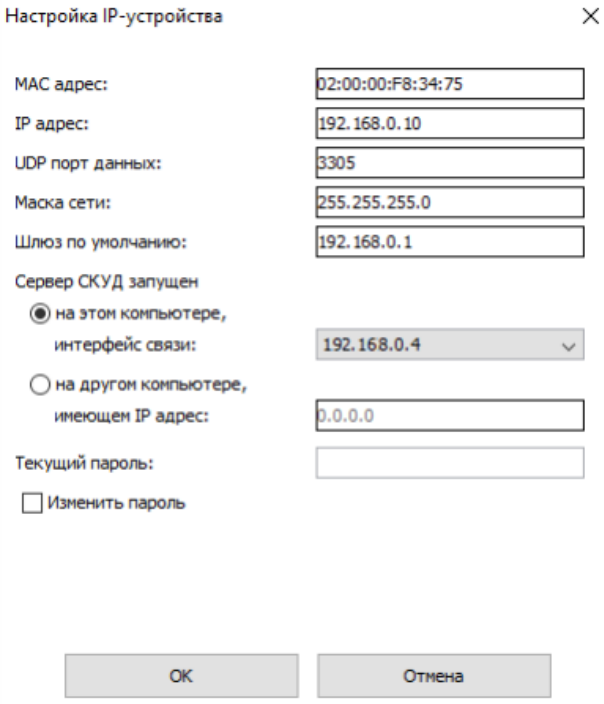
- Конфликт IP-адресов в сети. При отсутствии связи с контроллером на вкладке «Оборудование» в программе «Клиент» (контроллер при этом виден в списке «Найденные в сети IP-устройства» программы «Управление сервером» и может успешно отвечать на команду ping) рекомендуется выключить питание контроллера и 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.

- Некорректные настройки сетевых интерфейсов ОС. 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»).

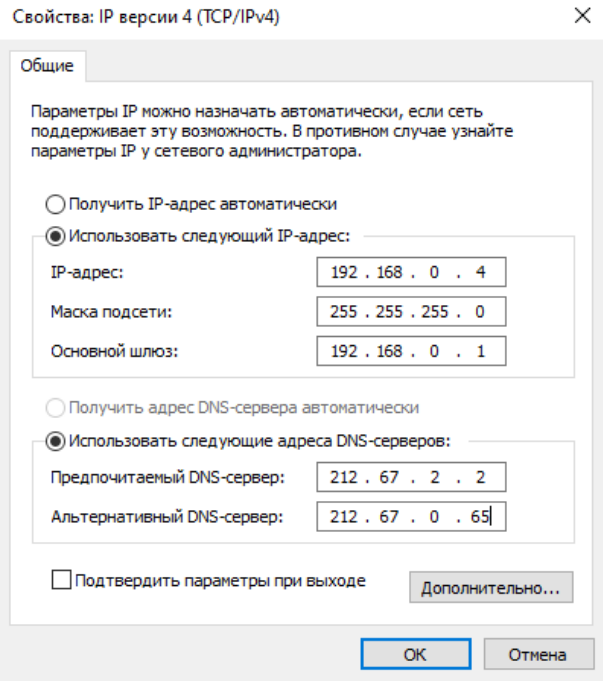


Неправильные настройки сетевого интерфейса для подключения контроллера.

Пример корректной настройки сервера и контроллера приведён ниже.



Пример правильной настройки контроллера.



Пример правильных настроек сетевого интерфейса сервера.

- 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:

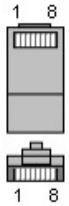


Рис. 39. Нумерация контактов разъёма RJ-45.

«Прямой» кабель для соединения с помощью коммутаторов.

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

12. Возможные сообщения об ошибках при запуске серверного модуля

12.1. 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

В Sigur реализовано шифрование трафика по протоколу TLS между частями системы для обеспечения безопасности передачи данных. Рекомендуется использовать встроенную функциональность шифрования для исключения возможности перехвата и утечки конфиденциальной информации.

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

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

По умолчанию используется незащищённое соединение. Выбор предпочтительного метода взаимодействия остаётся за пользователем системы. Функциональность шифрования данных не лицензируется и доступна в бесплатной версии ПО.

На текущий момент сервером Sigur поддерживаются TLS 1.2 и TLS 1.3. Клиентские рабочие места Sigur на Windows используют TLS 1.2, а рабочие места на Linux используют TLS 1.3.

Настройка шифрования между сервером и контроллерами Sigur по DTLS описана в отдельном разделе.

14.1. Переход на небезопасное соединение и запрет подключения к серверу

Шифрование данных по TLS отключено в системе по умолчанию.

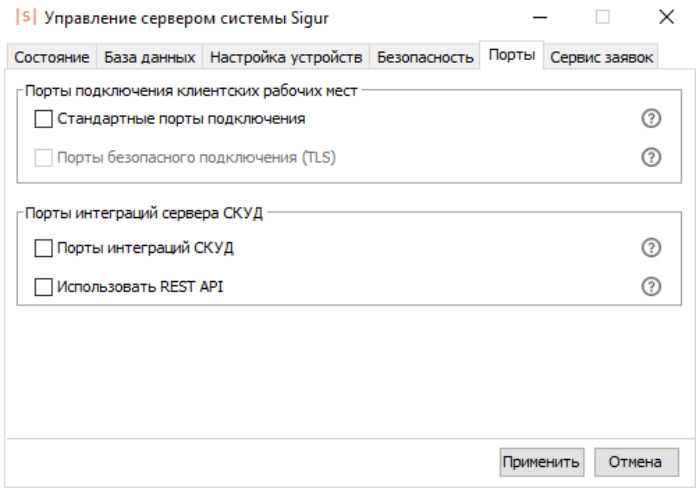
Пользователь может настроить параметры защищённого соединения, а также полностью или частично запретить подключение к сетевым портам сервера Sigur.

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

1. Активен только чекбокс «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 чекбокс «Стандартные порты подключения». Клиентские места Sigur могут использовать только незащищённое соединение при подключении к серверу. В стартовом меню ПО «Клиент» «Вход в систему» – «Выбор сервера» – «Параметры подключения» должен быть отключён чекбокс «Использовать безопасное подключение».
3. Активны оба чекбокса. Клиентские места Sigur могут использовать любой вид соединения, конфигурация каждого места настраивается отдельно.
4. Выключены оба чекбокса. 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 чекбоксы в блоке ПО «Управление сервером» – «Порты» – «Порты интеграций СКУД».



Пример полного запрета подключения к портам сервера Sigur.

Настройка безопасного соединения подробно описана в следующих разделах.

14.2. Установка зашифрованного соединения между клиентом и сервером

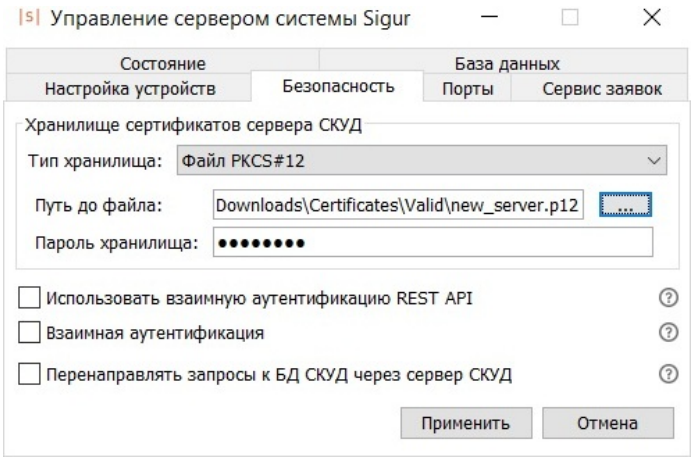
В данном разделе описан процесс настройки ПО Sigur для шифрования трафика между серверной и клиентской частями системы. Каждое клиентское рабочее место Sigur конфигурируется отдельно.

14.2.1. Настройка сервера Sigur

Для настройки серверной части СКУД необходимо:

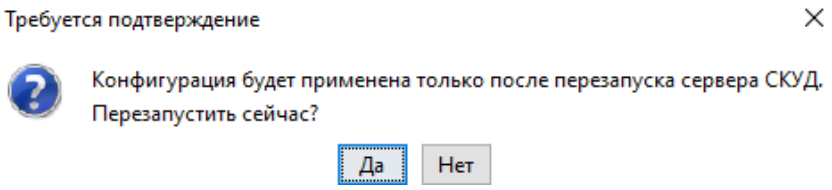
1. Подготовить хранилище сертификатов безопасности сервера. Ознакомиться с требованиями к файлу хранилища вы можете в разделе по этой ссылке.

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 одноимённых полях.



Вкладка «Безопасность» ПО «Управление сервером».

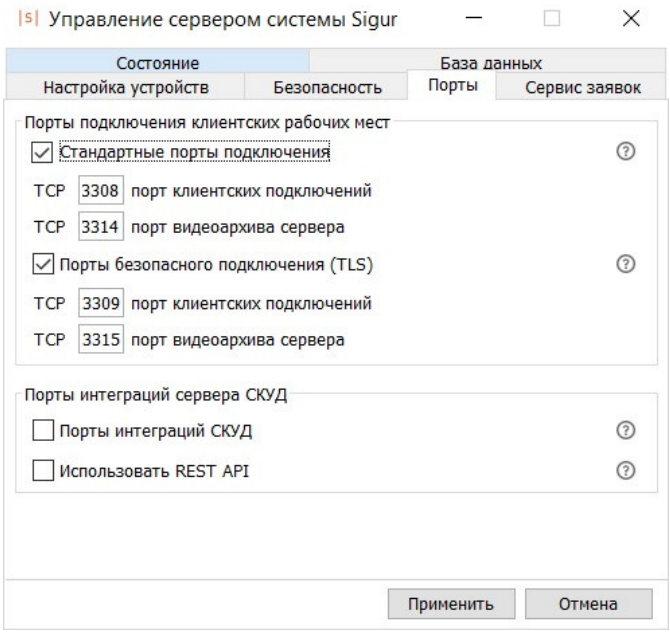
3. Нажать кнопку «Применить», после чего система выведет предупреждение о необходимости перезапуска серверного модуля для применения новой конфигурации. Перезапустите серверный модуль.



Предупреждение о необходимости перезапуска серверного модуля.

4. Указать порты для защищённого соединения. Для этого нужно перейти на вкладку «Порты» ПО «Управление сервером» и активировать чекбокс «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.

   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).



Вкладка «Порты» ПО «Управление сервером».

Порты, использующиеся системой, не должны дублироваться.

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

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.

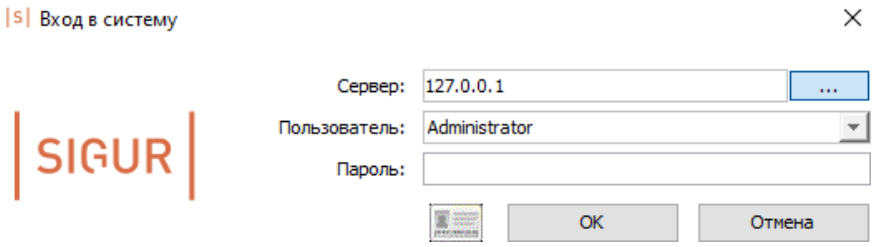
- Валидный сертификат сервера формата X.509. Срок действия сертификата не должен быть истекшим.
- Цепочку доверия сертификатов формата X.509.

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

14.2.3. Настройка клиентской части ПО Sigur

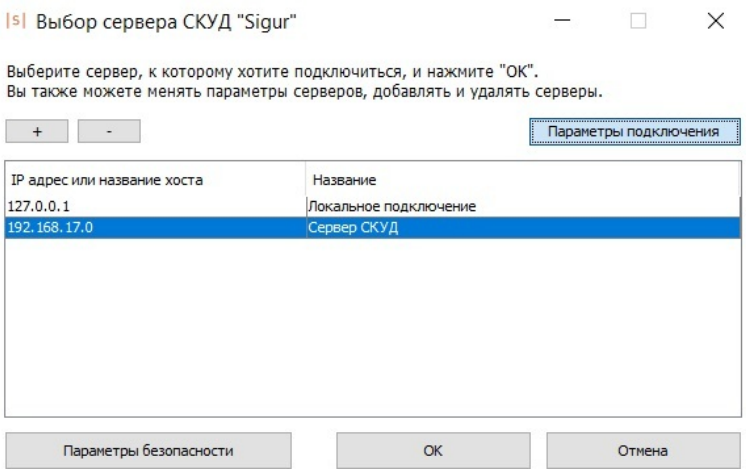
Требуется выполнить следующие настройки на каждом клиентском рабочем месте Sigur, которое будет устанавливать защищённое соединение с сервером:

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».



Окно «Вход в систему».

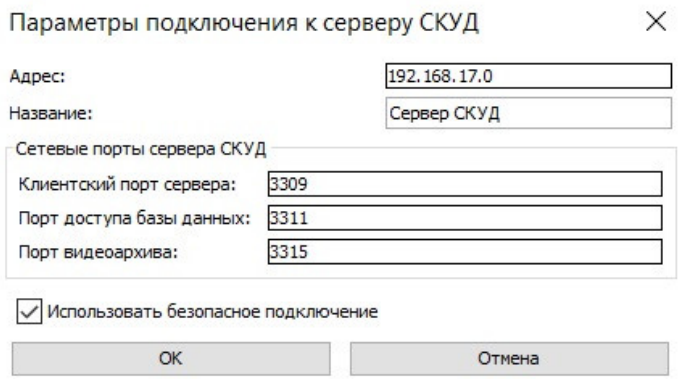
2. Далее необходимо ввести реквизиты соединения с новым сервером или выделить в списке ранее добавленный сервер и нажать кнопку «Параметры подключения».



Окно «Выбор сервера СКУД Sigur».

3. В окне «Параметры подключения к серверу СКУД» нужно активировать чекбокс «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 «OK».



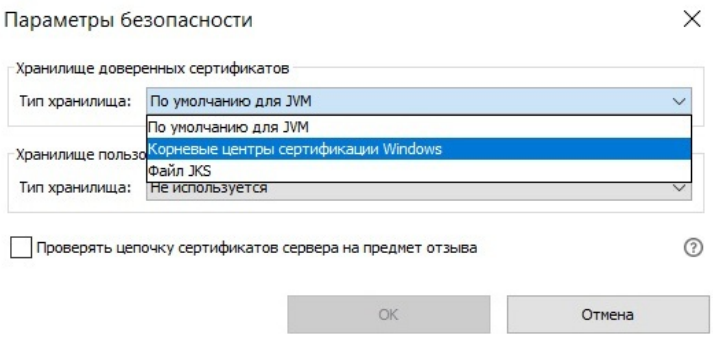
Окно «Параметры подключения к серверу СКУД».

   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.

4. 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 (Java KeyStore). Доступен на ОС Windows и Linux. Файл должен содержать доверенные корневые сертификаты.
   - Файл PKCS#12. Доступен на ОС Linux. Файл должен содержать доверенные корневые сертификаты.

   Для сохранения настроек необходимо нажать кнопку «OK».



Окно «Параметры безопасности».

На этом настройка защищённого 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 защищённое 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.

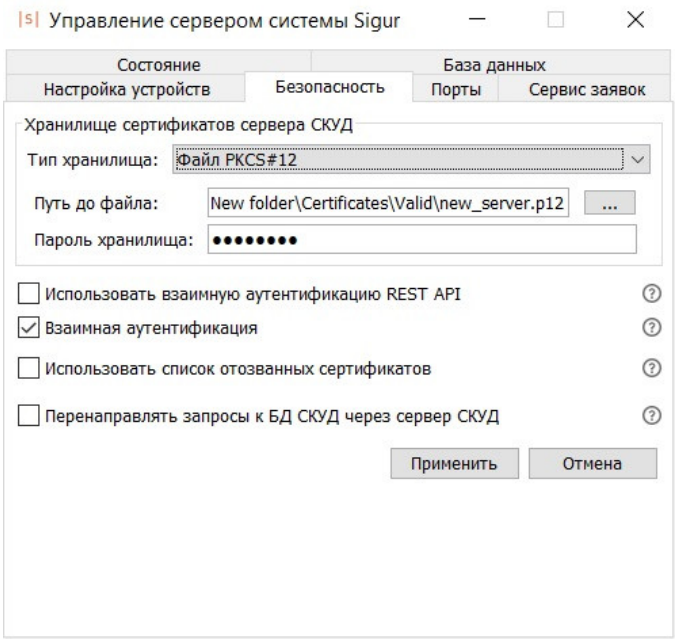
При использовании автоматического входа в ПО Sigur (автологин) система оперирует параметрами подключения и безопасности пользователя операционной системы, от имени которого осуществляется вход. Клиентское рабочее место должно быть соответствующим образом сконфигурировано перед использованием автоматического входа в систему.

14.3. Взаимная аутентификация

В дополнение к проверке сертификата сервера возможно активировать функционал взаимной аутентификации (mTLS). 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:

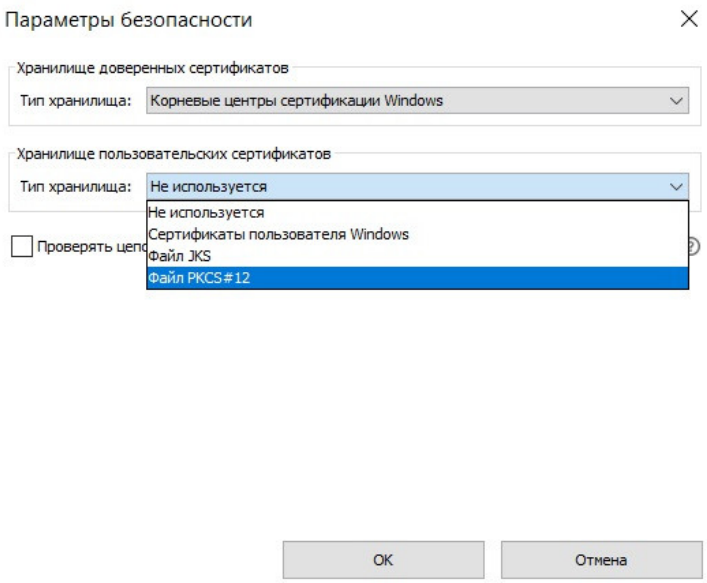
1. Сконфигурировать серверную часть Sigur аналогично инструкции в разделе «Настройка сервера Sigur».
2. Включить чекбокс «Взаимная аутентификация» на вкладке «Безопасность» ПО «Управление сервером».



Чекбокс «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 стартовом меню ПО «Клиент» «Вход в систему» – «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 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.
- 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.

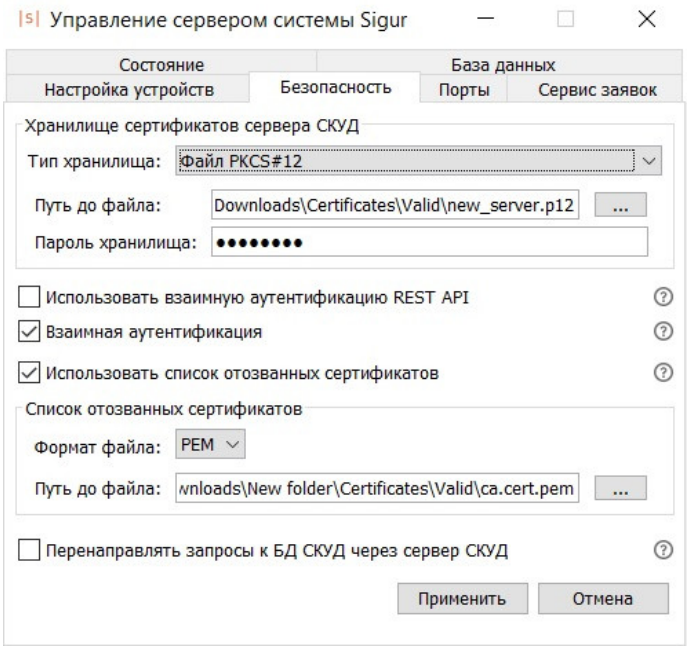
14.4. Проверка статуса отзыва сертификата

В системе доступна функциональность 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 функциональности необходимо:

1. Включить чекбокс «Взаимная аутентификация» на вкладке «Безопасность» ПО «Управление сервером».
2. Включить ставший доступным чекбокс «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 функциональности необходимо в стартовом меню ПО «Клиент» «Вход в систему» – «Выбор сервера СКУД Sigur» – «Параметры безопасности» включить чекбокс «Проверять цепочку сертификатов сервера на предмет отзыва». 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.

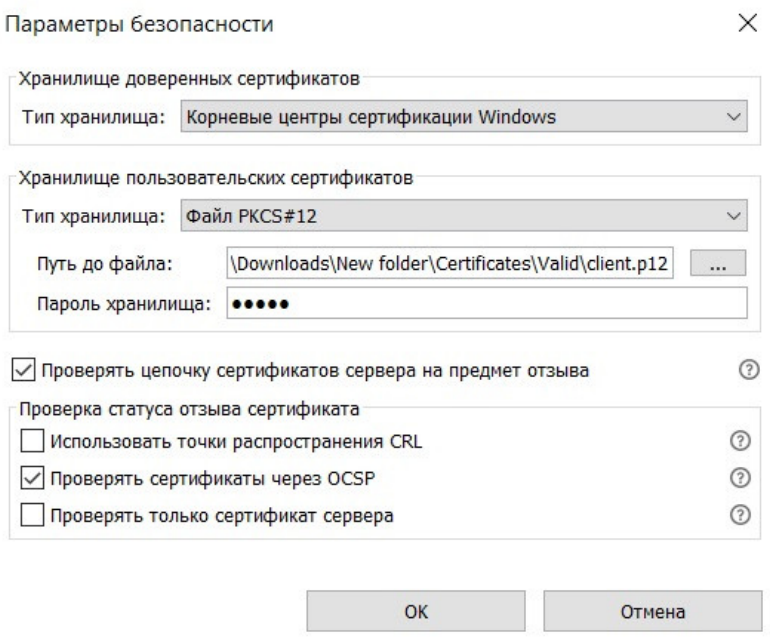
2. Проверять сертификаты через OCSP. Предпочтительный вариант. Система будет отправлять запрос на OCSP-сервер для проверки отзыва сертификата сервера Sigur или цепочки сертификатов. URI OCSP-сервера должен быть явно прописан в атрибуте Authority Information Access X509v3 extension сертификата (сертификатов),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

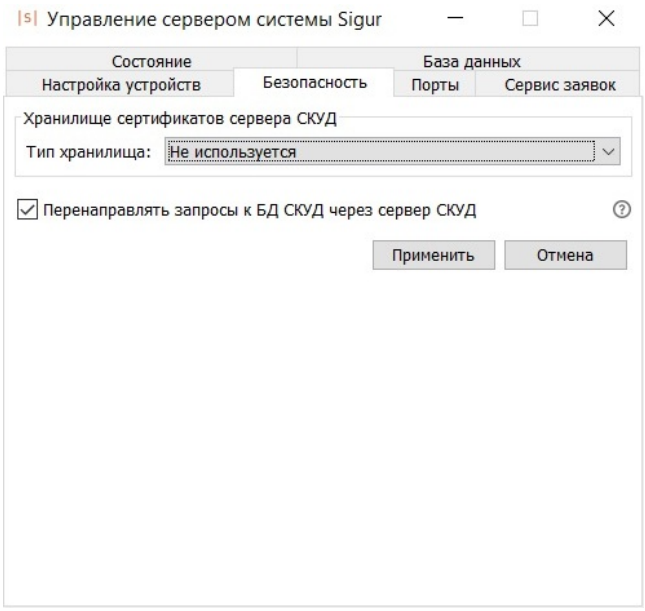
- Перенаправлять запросы к БД через сервер без использования TLS-шифрования. Это исключает возможность прямого подключения клиентских мест к БД СКУД.
- Перенаправлять запросы к БД через сервер совместно с шифрованием трафика по TLS. Таким образом обеспечивается максимальная защита данных в системе.

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:

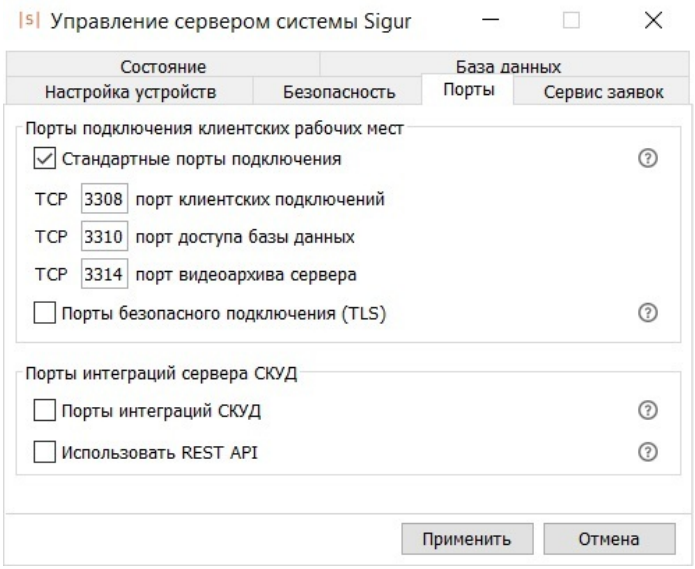
- Включить чекбокс «Перенаправлять запросы к БД СКУД через сервер СКУД» на вкладке «Безопасность» ПО «Управление сервером».



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 соответствующем разделе.

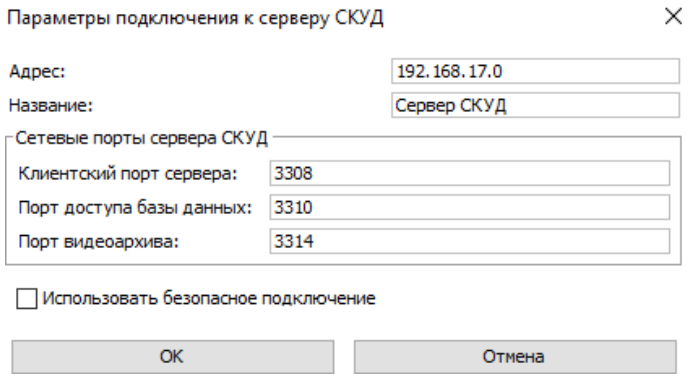


Настройка портов сервера при незащищённом соединении.

- Повторно сохранить настройки и перезапустить серверный модуль.

2. Конфигурирование клиентского рабочего места Sigur:

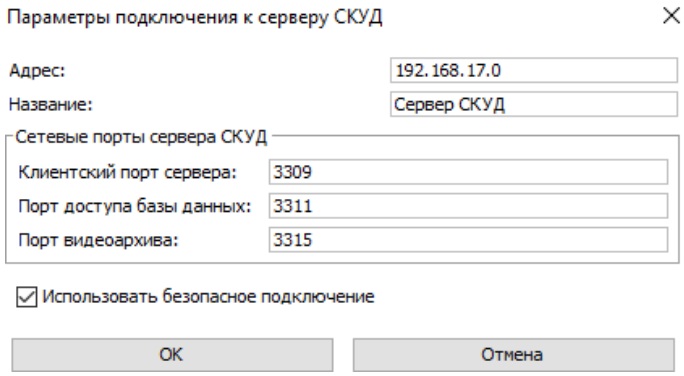
- Задать порт для подключения к базе данных в стартовом меню ПО «Клиент» «Вход в систему» – «Выбор сервера СКУД Sigur» – «Параметры подключения» – «Параметры подключения к серверу СКУД». Номер порта должен соответствовать порту, заданному ранее в настройках серверной части ПО.



Порты подключения клиента 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 соответствующем разделе.



Порты подключения к серверу при защищённом соединении.

Функциональность перенаправления запросов к базе данных также совместима 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.

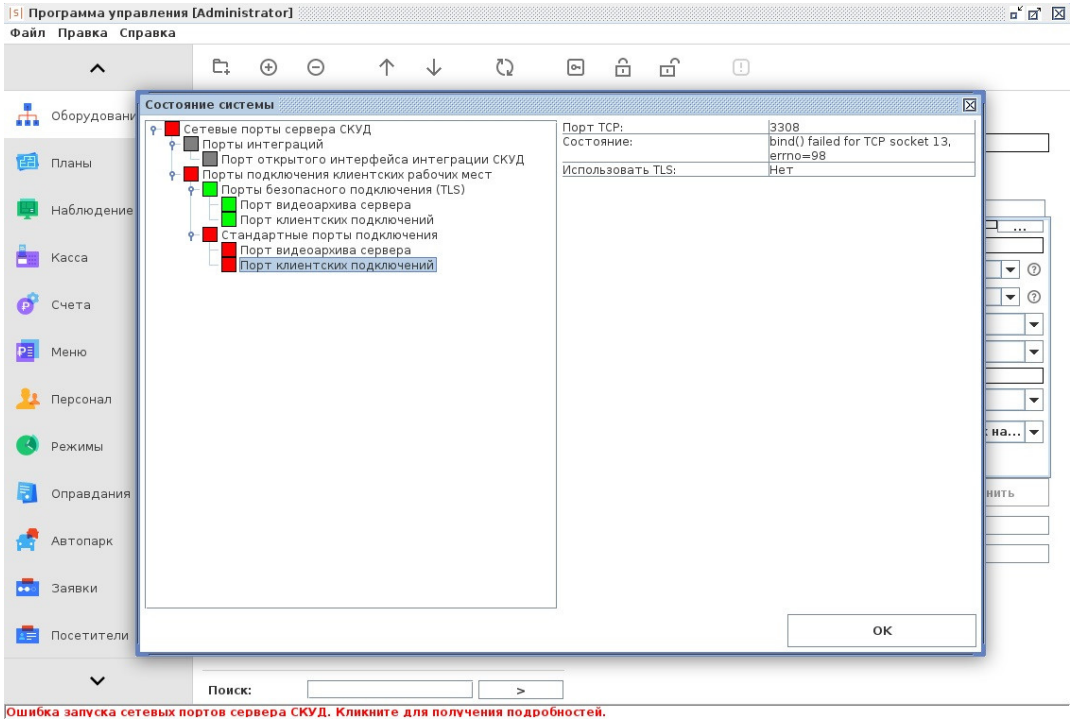
Информация о необходимых настройках размещена в отдельных руководствах для данных интеграций.

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. Шифрование трафика между сервером и контроллерами по DTLS

В Sigur реализовано шифрование трафика между сервером и контроллерами по протоколу DTLS 1.2. Функциональность не лицензируется и доступна в бесплатной версии ПО.

Чтобы уточнить, поддерживает ли конкретная модель контроллера DTLS, обратитесь к руководству по эксплуатации контроллера.

По умолчанию шифрование данных по DTLS отключено. В данном разделе описан процесс настройки защищённого соединения между сервером и контроллерами. Настройка системы осуществляется в два этапа:

1. Создание профилей шифрования.
2. Назначение профилей контроллерам и серверу.

Настройку можно производить с любого рабочего места Sigur, подключённого к необходимому серверу СКУД.

15.1. Порядок взаимодействия сервера и контроллеров

По умолчанию контроллеры обмениваются данными с сервером без шифрования по порту UDP 3305. Во время первого применения профиля шифрования на контроллер передаются его приватный ключ и сертификат в незашифрованном виде.

Чтобы исключить риск перехвата сертификатов и приватных ключей контроллеров, необходимо обеспечить изолированность системы при первоначальной загрузке профилей шифрования.

После получения профиля шифрования контроллер пытается построить тестовую DTLS-сессию по порту UDP 3306 сервера.

В случае успеха профиль шифрования считается применённым, и дальнейшее защищённое взаимодействие с сервером осуществляется по порту UDP 3307.

Если тестовая сессия не будет установлена, обмен данными продолжится в прежнем режиме: без шифрования по порту UDP 3305 или с использованием предыдущего сертификата.

При изменении профиля шифрования контроллера новый сертификат и ключ передаются по ранее зашифрованному каналу связи.

15.2. Создание профилей шифрования

Перед установкой зашифрованного соединения необходимо создать профиль шифрования – правило предоставления, проверки и генерации сертификатов контроллеров. Для этого:

1. Запустите ПО «Клиент» и перейдите в меню «Файл» – «Настройки» – «Профили шифрования».

2. Нажмите кнопку «+».

3. В открывшемся окне введите имя профиля (названия не должны повторяться) и выберите его тип:

- **Автоматически созданный профиль**. Сервер СКУД создаст самоподписанный корневой CA-сертификат и его приватный ключ. Они будут использоваться при генерации сертификатов для сервера и контроллеров.

  Сервер генерирует приватные RSA-ключи стандарта PKCS#8 без шифрования с длиной ключа в 2048 бит. Формат всех сертификатов – X.509 с алгоритмом подписи SHA256. Срок действия сертификатов – 3 года.

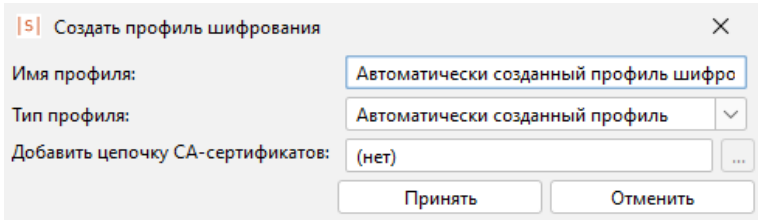
- **Пользовательский профиль**. Необходимо вручную загрузить корневой CA-сертификат, либо цепочку, включающую корневой сертификат и до двух промежуточных сертификатов, а также сертификаты для сервера и контроллеров. Поддерживаются:

  - Приватные RSA-ключи длиной 2048 и 4096 бит включительно в формате PEM стандарта PKCS#8 без шифрования. Доступ к приватному ключу осуществляется без пароля.

  - Сертификаты в формате PEM стандарта X.509 с алгоритмом подписи SHA256. Загружаемый сертификат должен содержать расширение Basic Constraints. Поле Subject загружаемого сертификата не должно полностью совпадать с полем Subject CA-сертификата. Срок действия сертификата не должен быть истекшим. Если срок действия ещё не наступил, сертификат можно загрузить и добавить в профиль, но его применение на контроллере будет недоступно.

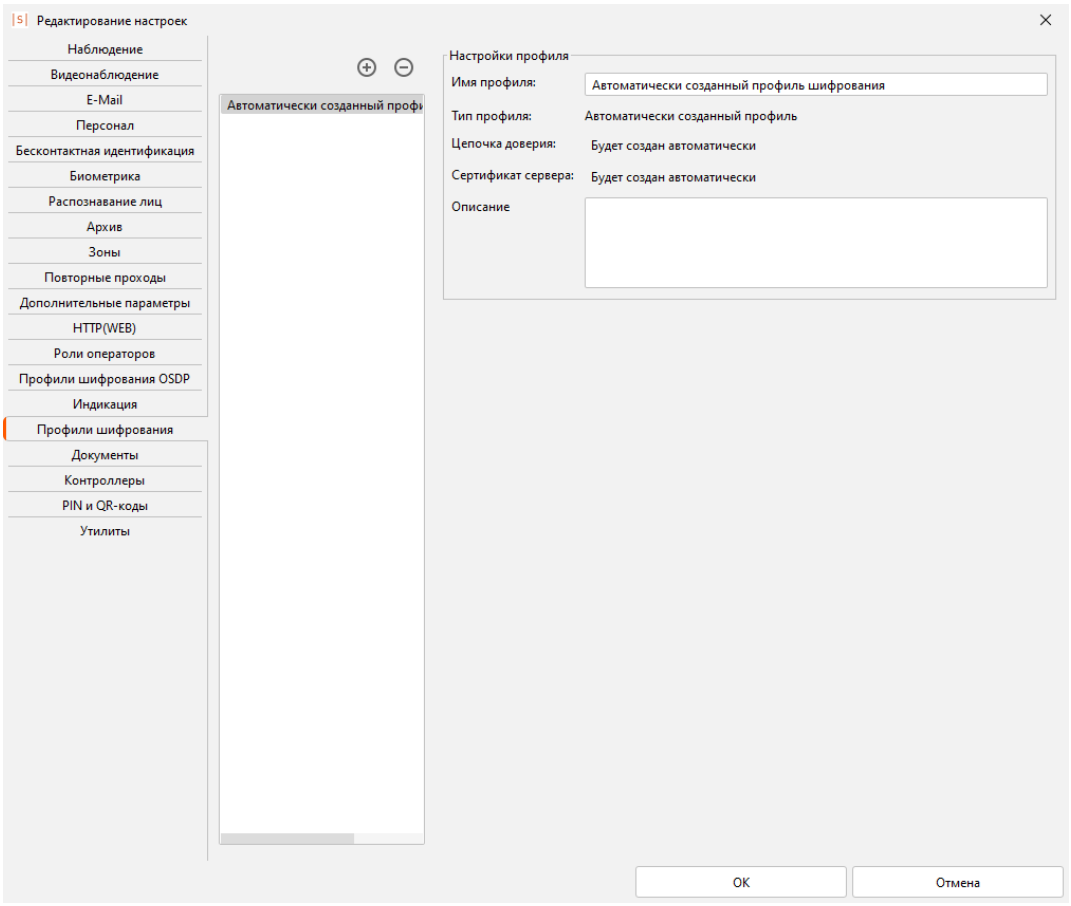
Выбор типа профиля шифрования определяется требованиями информационной безопасности на объекте, наличием центра сертификации и другими факторами.

4.1. Если необходим автоматически созданный профиль, нажмите «Принять».



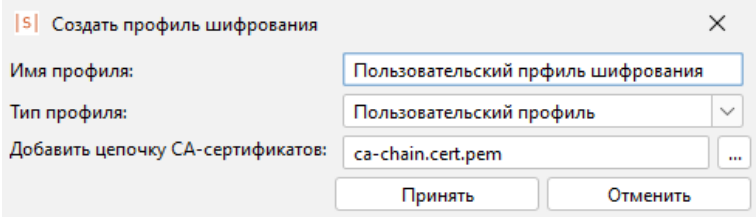
Создание профиля шифрования.

4.2. Добавьте произвольное описание (если требуется) и завершите создание профиля, нажав «ОК». После этого будут созданы корневой CA-сертификат и сертификат сервера СКУД. Сертификаты для контроллеров генерируются сервером автоматически при применении профиля.



Настройка автоматически созданного профиля шифрования.

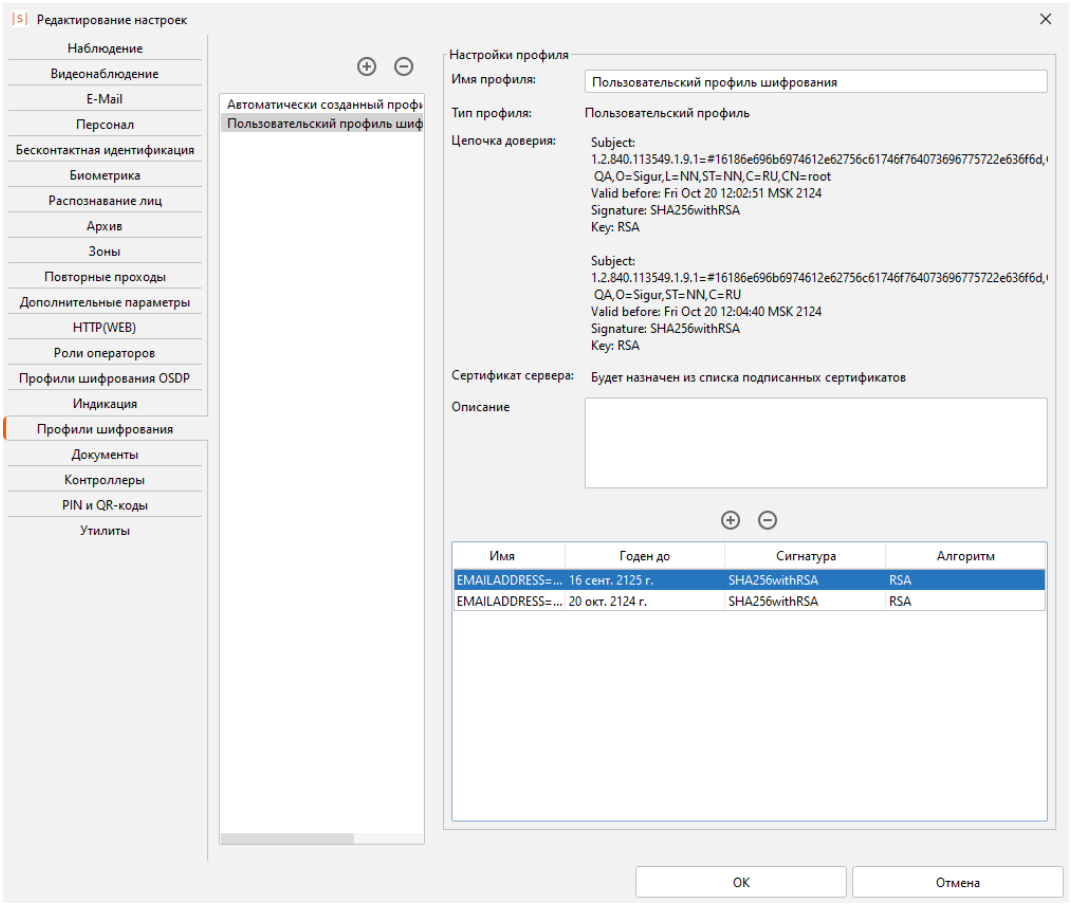
5.1. При выборе пользовательского профиля необходимо сначала добавить корневой CA-сертификат. Для этого нажмите кнопку «...», выберите нужный файл и нажмите «Принять».



Создание профиля шифрования.

5.2. Затем с помощью кнопки «+» добавьте в профиль шифрования SSL-сертификаты вместе с их приватными ключами. Необходимо загрузить один сертификат для сервера и по одному сертификату для каждого контроллера. Все сертификаты должны быть подписаны корневым CA, указанным на предыдущем этапе.

Обратите внимание: в качестве сертификата сервера автоматически будет использован последний сертификат в списке.

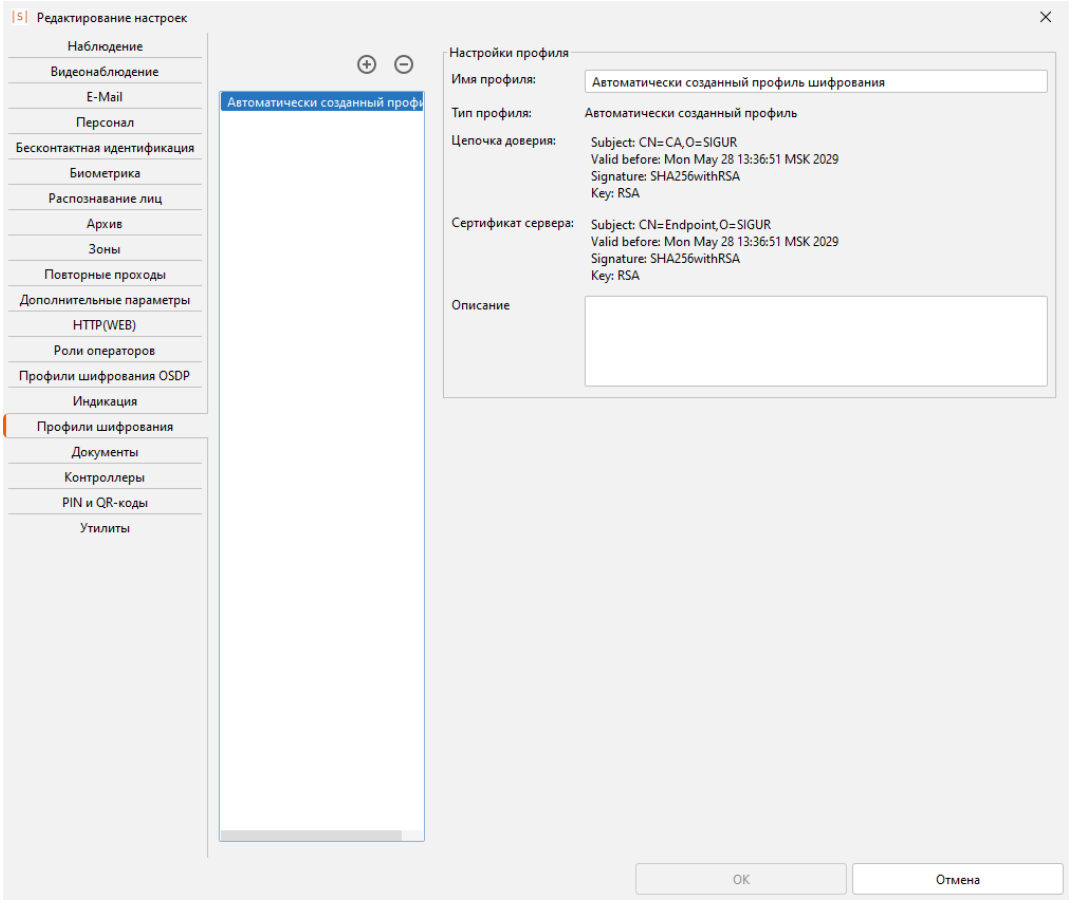


Настройка пользовательского профиля шифрования.

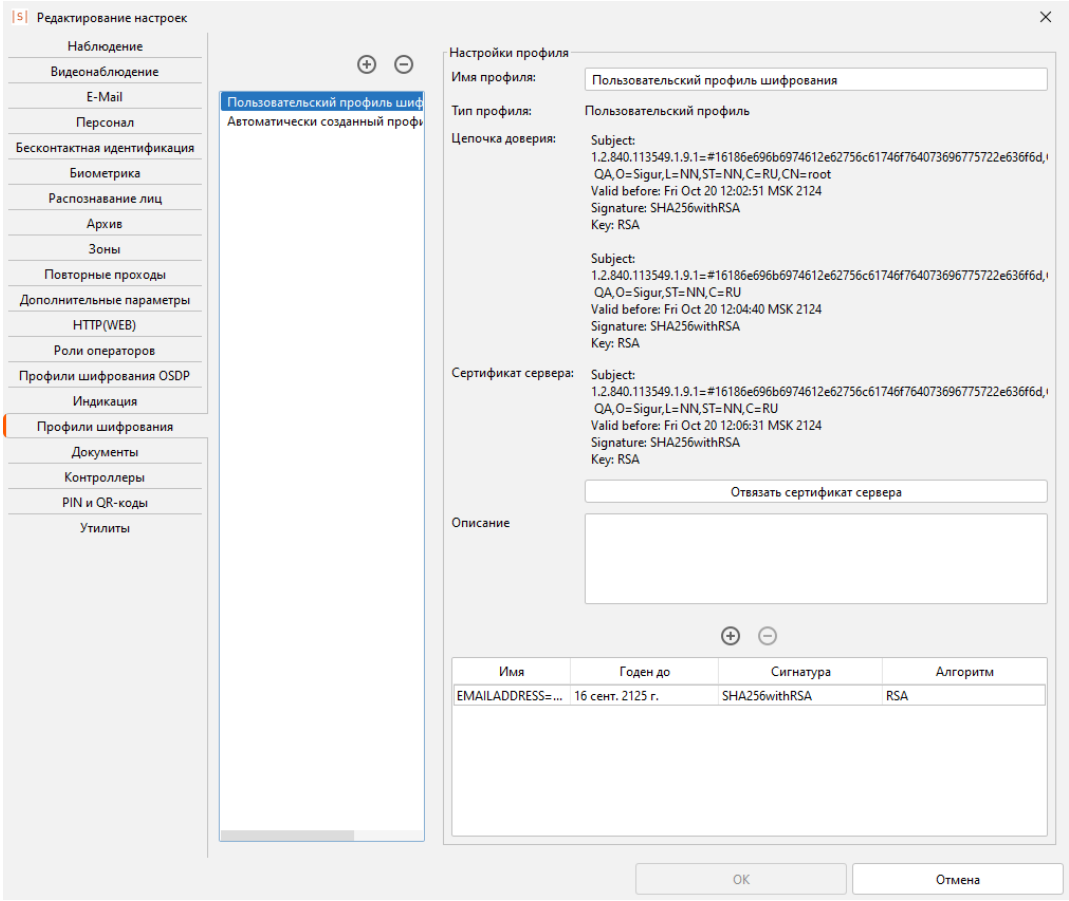
5.3. При необходимости добавьте описание профиля и завершите его создание, нажав «ОК». После этого последний сертификат в списке станет сертификатом сервера, а остальные останутся в профиле для последующего применения на контроллеры.

Сертификаты контроллеров будут автоматически удаляться из профиля после его применения, вне зависимости от успешности попытки. В дальнейшем вы можете добавлять новые сертификаты контроллеров в пользовательский профиль шифрования.

6. Информацию о созданных профилях можно просмотреть при повторном входе в меню «Файл» – «Настройки» – «Профили шифрования».



Автоматически созданный профиль шифрования.



Пользовательский профиль шифрования.

При необходимости профиль можно удалить с помощью кнопки «-». Если профиль уже назначен контроллеру, появится дополнительное предупреждение. После удаления назначенного профиля необходимо применить новый или выполнить сброс настроек шифрования.

В пользовательском профиле доступна кнопка «Отвязать сертификат сервера» – она используется при замене или истечении срока действия серверного сертификата. Подробнее см. в разделе «Применение профилей шифрования».

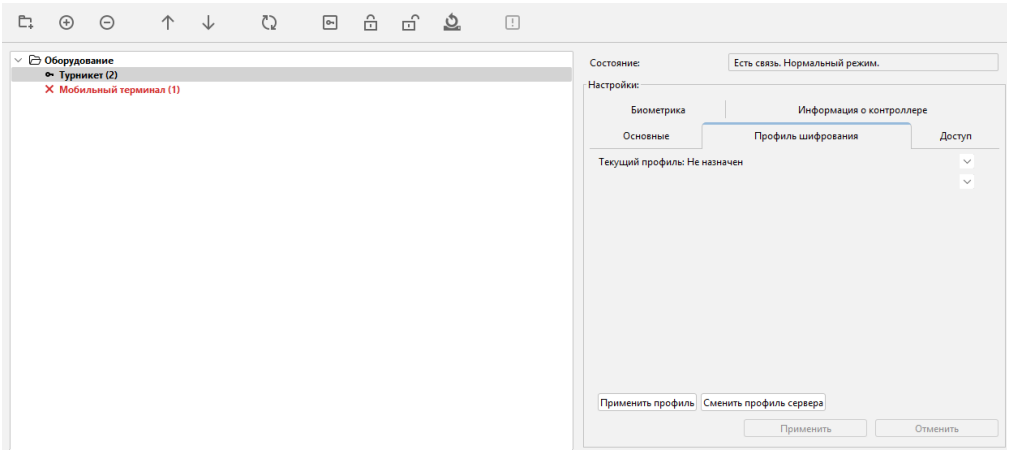
15.3. Применение профилей шифрования

Созданный профиль шифрования необходимо применить к серверу и контроллерам. Для этого:

1. Перейдите на вкладку «Оборудование» ПО «Клиент» и выделите в списке точку доступа, относящуюся к необходимому контроллеру. Для массового применения профиля выделите каталог или несколько точек доступа в списке с помощью клавиш Ctrl или Shift.

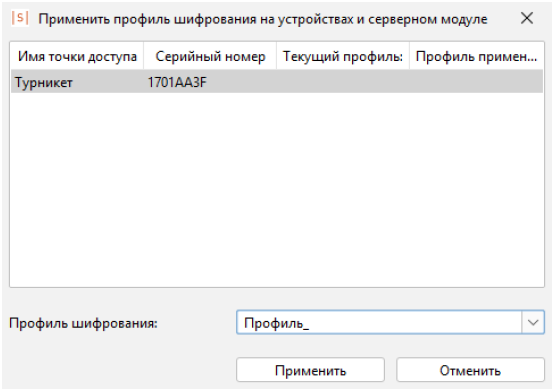
2. Убедитесь, что с контроллером установлена связь, а в сети разрешён обмен UDP-пакетами по портам UDP 3305, 3306, 3307.

3. Откройте подвкладку «Профиль шифрования» и нажмите кнопку «Применить профиль». При этом выбранный профиль шифрования будет применён одновременно на стороне сервера СКУД и контроллера.



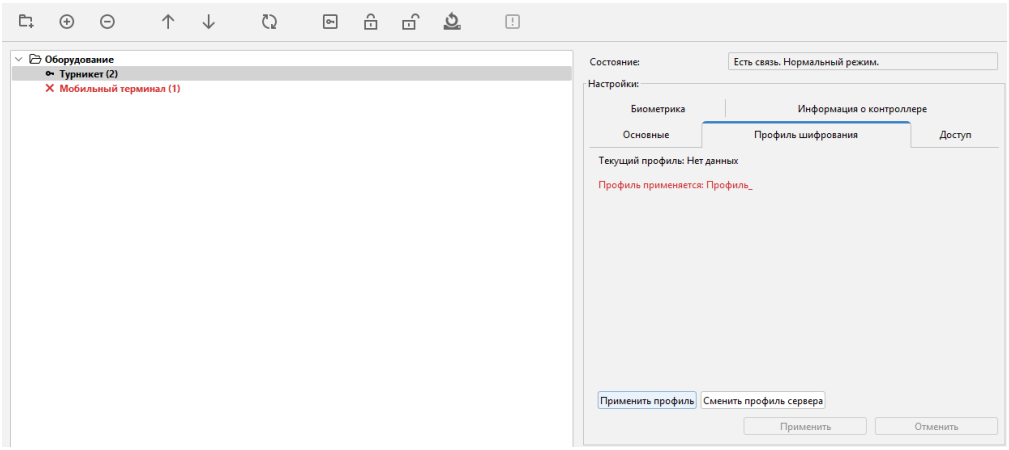
Профиль шифрования не назначен.

4. В открывшемся окне выберите необходимый профиль шифрования из выпадающего списка и нажмите «Применить».



Выбор профиля шифрования.

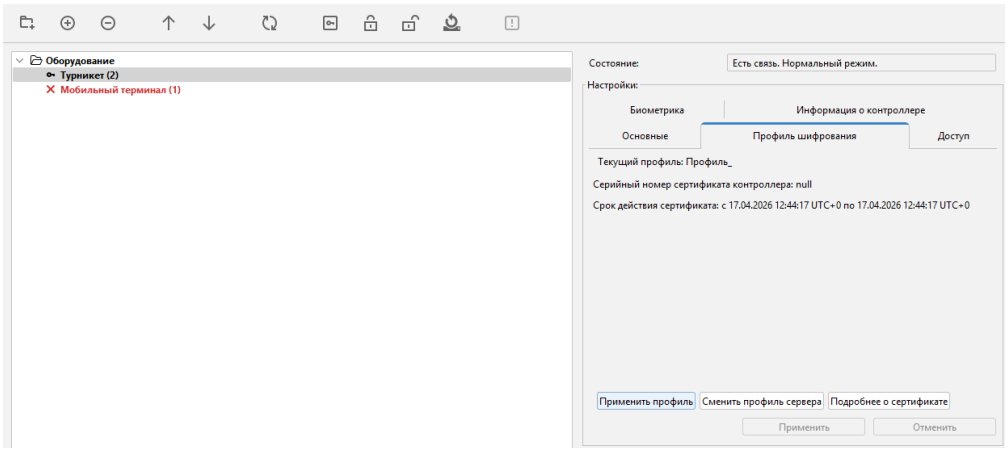
5. Система начнёт применение профиля к контроллеру. Информация о процессе и текущем профиле отображается на подвкладке «Профиль шифрования».



Применение профиля шифрования.

6. После завершения операции в интерфейсе отобразится информация о применённом профиле шифрования контроллера.

При использовании пользовательского профиля сертификаты для контроллеров будут удалены из профиля после попытки записи на устройство, независимо от результата.



Профиль шифрования применён.

Если в процессе применения профиля возникнет ошибка, система отобразит соответствующее сообщение. Например, ошибка может возникнуть из-за сетевых проблем (закрыт необходимый порт) или если в пользовательском профиле шифрования не хватило сертификатов для всех выбранных контроллеров.

Профиль шифрования не будет применён, если:

- Срок действия корневого или серверного сертификата ещё не наступил.
- Истёк срок действия сертификата сервера. В этом случае он будет удалён из профиля. Если был выбран пользовательский профиль шифрования, сервер получит последний сертификат из оставшихся в профиле. Изменения применятся после перезапуска серверного модуля.
- Истёк срок действия корневого сертификата – профиль шифрования будет полностью удалён.
- В профиле отсутствует сертификат сервера или контроллера.

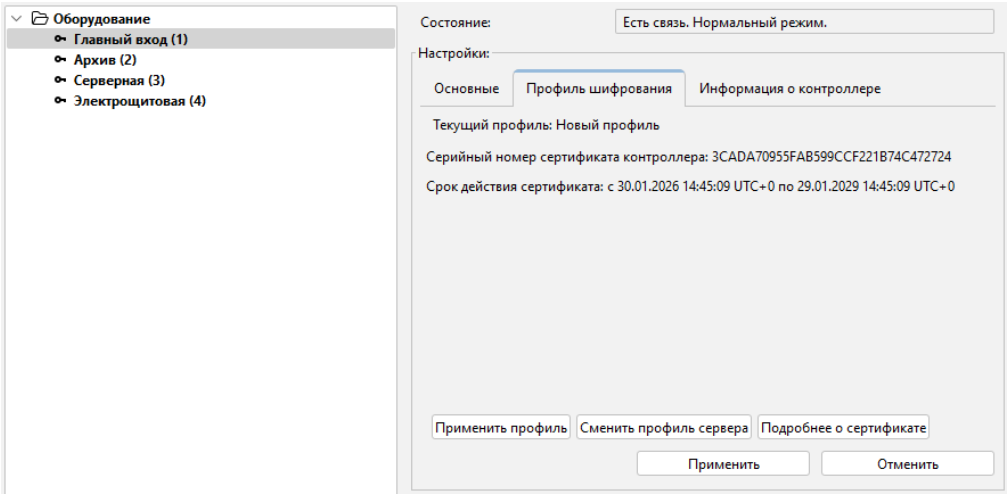
Во всех случаях система выводит поясняющее сообщение об ошибке.

Смена профиля шифрования на стороне сервера.

В системе предусмотрена возможность смены профиля шифрования только на стороне сервера без его загрузки на контроллер. Для этого:

1. Перейдите на вкладку «Оборудование» ПО «Клиент» и выделите в списке точку доступа, относящуюся к необходимому контроллеру. Для массового применения профиля выделите каталог или несколько точек доступа в списке с помощью клавиш Ctrl или Shift.
2. Откройте подвкладку «Профиль шифрования» и нажмите кнопку «Сменить профиль сервера».
3. В открывшемся окне выберите необходимый профиль шифрования из выпадающего списка и нажмите «Применить».

При выполнении операции профиль шифрования изменяется только на стороне сервера СКУД и не затрагивает профиль, применённый на контроллере.



Вкладка «Оборудование» – «Профиль шифрования».

Функция применяется, например, при безопасном вводе контроллера в эксплуатацию без передачи приватного ключа по незащищённому каналу.

Рассмотрим пример такого сценария:

1. На основном сервере СКУД созданы два профиля шифрования: инсталляционный (временный) и основной. Оба профиля используют одну и ту же цепочку доверия.
2. Инсталляционный профиль загружается на контроллер на этапе монтажа (например, с другого сервера СКУД) с помощью кнопки «Применить профиль».
3. На основном сервере СКУД сконфигурирована точка доступа с серийным номером данного контроллера.
4. К точке доступа применяется инсталляционный профиль шифрования с помощью кнопки «Сменить профиль сервера». В результате на основном сервере СКУД используется профиль, совпадающий с профилем, ранее загруженным на контроллер.
5. Контроллер подключается в целевую сеть и устанавливает DTLS-сессию с основным сервером СКУД, используя инсталляционный профиль.
6. После установления защищённого соединения оператор применяет основной профиль шифрования к серверу и контроллеру с помощью кнопки «Применить профиль». Таким образом, сертификат и приватный ключ контроллера передаются поверх существующей DTLS-сессии.

Обновление сертификатов.

Если срок действия сертификатов в применённом профиле истёк, новый профиль можно применить только после сброса настроек шифрования.

Исключение составляет случай истечения срока действия сертификата сервера в пользовательском профиле шифрования. Для его замены:

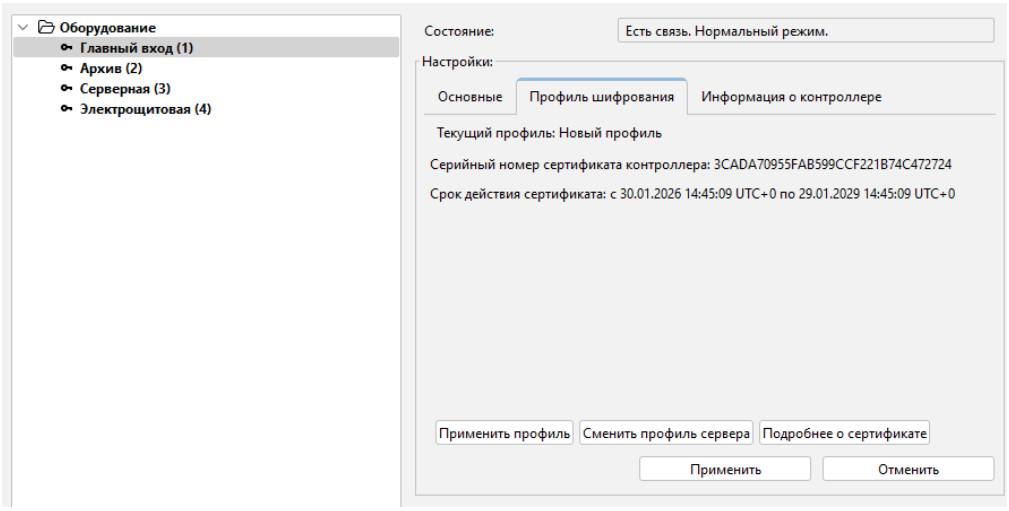
1. Перейдите в раздел «Файл» – «Настройки» – «Профили шифрования».
2. Выберите нужный профиль и нажмите кнопку «Отвязать сертификат сервера» (сертификат вернётся в общий список).
3. Удалите устаревший сертификат, добавьте новый и сохраните изменения кнопкой «ОК».

Новые настройки вступят в силу после перезапуска серверного модуля.

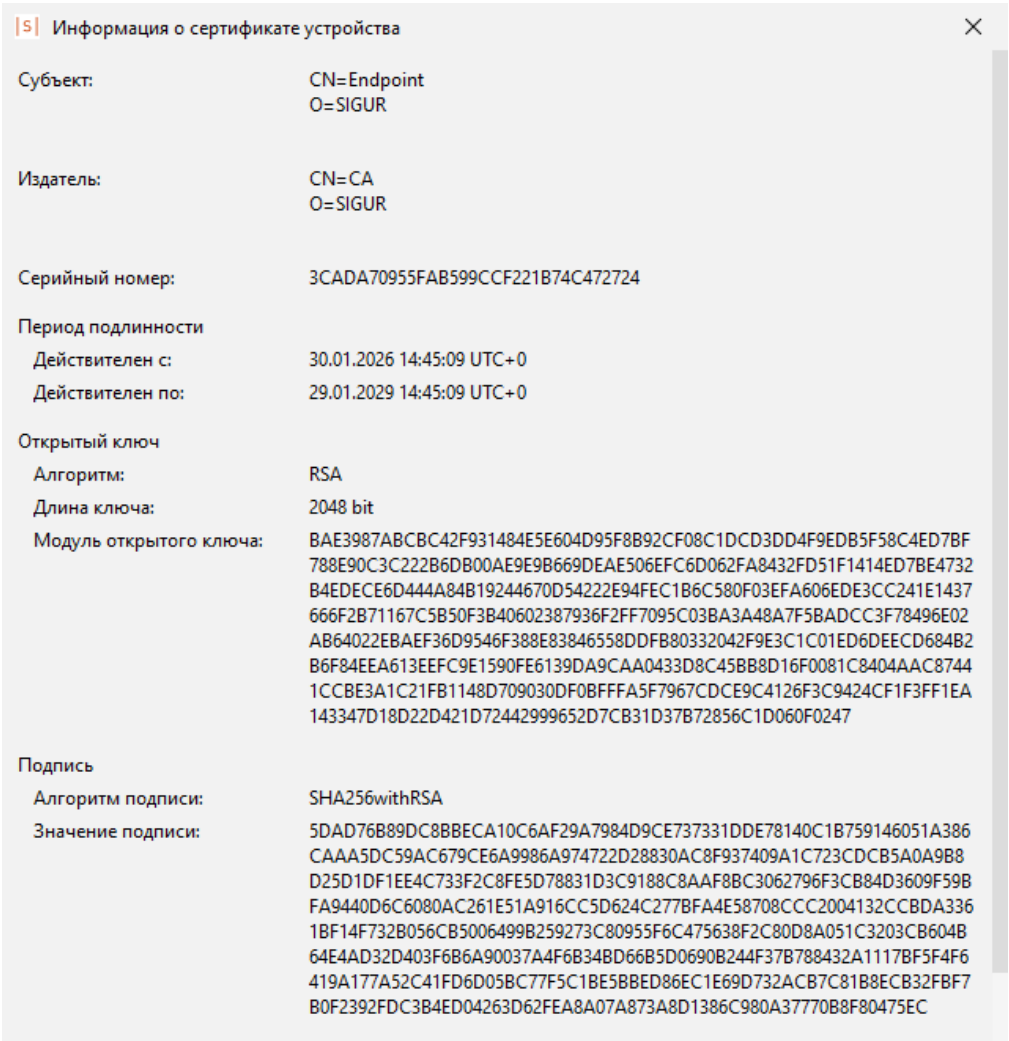
15.4. Просмотр информации о сертификате шифрования контроллера

Если на контроллере применён профиль шифрования DTLS, то на вкладке «Оборудование» ПО «Клиент» можно просматривать информацию о сертификате, загруженном на контроллер.

Для этого выделите в списке точку доступа необходимого контроллера и раскройте подвкладку «Профиль шифрования». Здесь отображаются название профиля, серийный номер сертификата контроллера и срок его действия. Далее нажмите кнопку «Подробнее о сертификате» – откроется окно с подробной информацией о сертификате устройства.



Вкладка «Оборудование» – «Профиль шифрования».



Информация о сертификате контроллера.

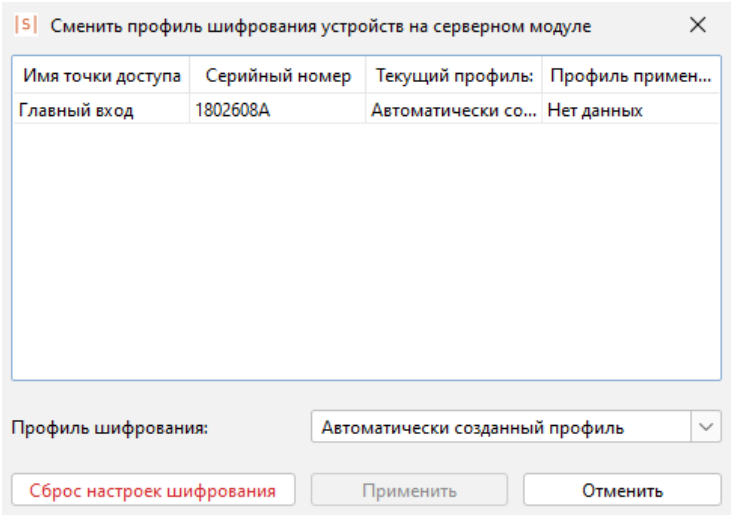
15.5. Сброс настроек шифрования и переход на незащищённое соединение

Для перехода на незащищённое соединение необходимо сбросить профиль шифрования как на контроллере, так и на сервере. Сброс можно выполнять в любом порядке.

Чтобы сбросить профиль шифрования на контроллере, для микропрограмм версий 0.x.x необходимо выполнить сброс и повторную настройку IP-параметров, а для микропрограмм версий 1.x.x и выше – аппаратный сброс. Инструкцию по сбросу см. в руководстве на соответствующую модель контроллера.

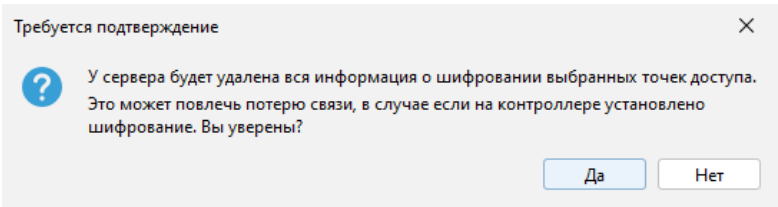
Для сброса профиля на сервере:

1. Перейдите на вкладку «Оборудование» ПО «Клиент» и выделите в списке точку доступа, относящуюся к необходимому контроллеру. Для массового сброса профилей выделите каталог или несколько точек доступа в списке с помощью клавиш Ctrl или Shift.
2. Раскройте вкладку «Профиль шифрования» и нажмите кнопку «Сменить профиль сервера».
3. В открывшемся окне нажмите кнопку «Сброс настроек шифрования».



Сброс настроек шифрования.

4. Подтвердите сброс, нажав «Да» в открывшемся окне.



Подтверждение сброса.

16. Мониторинг состояния контроллера с использованием SNMP

Контроллеры Sigur предоставляют возможность отслеживать их состояние с помощью протокола SNMP.

Чтобы уточнить, поддерживает ли конкретная модель контроллера SNMP, обратитесь к руководству по эксплуатации контроллера.

Контроллеры Sigur могут сообщать следующие параметры:

- серийный номер контроллера;
- локальная дата и время;
- внутренняя температура контроллера;
- напряжение питания контроллера;
- состояние OSDP считывателей (только контроллеры E2 и E4);
- состояние шлейфа пожарной сигнализации;
- состояние источника питания контроллера;
- состояние внешней АКБ (только контроллеры E2 и E4);
- состояние датчика открытия корпуса контроллера;
- состояние входных/выходных портов (контактов) контроллера.

Также контроллер может передать по SNMP протоколу Trap-сообщение с информацией о следующих событиях:

- срабатывание пожарной сигнализации;
- выход напряжения питания контроллера за пределы нормальных значений;
- открытие корпуса контроллера;
- изменение типа питания контроллера (от сети/от АКБ);
- потеря связи с OSDP считывателем (только контроллеры E2 и E4);
- иные зарегистрированные контроллером события (факты проходов, запретов доступа, тревоги и пр.).

Для настройки SNMP и мониторинга параметров устройств можно использовать специализированные инструменты, такие как SNMP Manager, Nagios, Zabbix, Cacti, Icinga. Они предоставляют удобный интерфейс для настройки и мониторинга SNMP.

16.1. Настройка взаимодействия по SNMP

16.1.1. Настройка контроллера

Для обеспечения взаимодействия по протоколу SNMPv3 необходимо провести настройку контроллера в программе «Управление сервером»: задать имя пользователя, пароль авторизации и шифрования, порт подключения.

Имя пользователя и пароль авторизации позволяют агенту SNMP проверять подлинность запросов от менеджера SNMP и определять, имеет ли пользователь право выполнять определённые действия. Пароль шифрования обеспечивает конфиденциальность данных, передаваемых между менеджером и агентом SNMP.

По умолчанию UDP-порт, на который SNMP-менеджер будет отправлять запрос на получение параметров контроллера – 161.

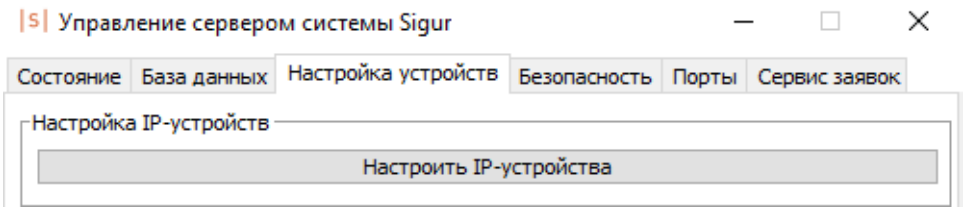
Отправка Trap-сообщений от контроллера Sigur осуществляется по SNMPv2. Здесь необходимо указать IP адрес SNMP сервера, который будет получать от контроллера Trap-сообщения.

По умолчанию UDP-порт SNMP-менеджера, на который контроллер будет отправлять trap-сообщения – 162.

Алгоритм настройки контроллера для взаимодействия по протоколу SNMP.

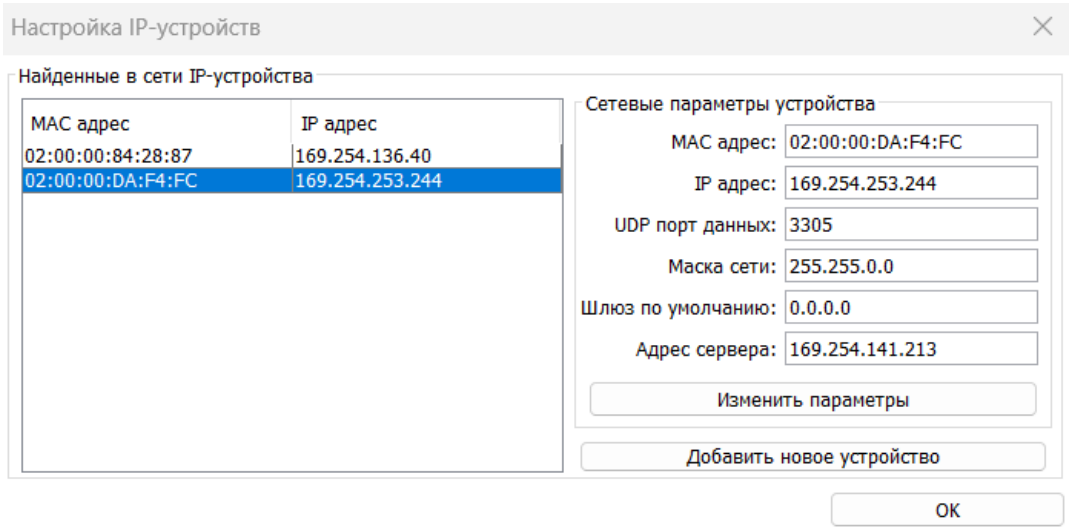
На вкладке «Настройка устройств» ПО «Управление сервером» можно производить настройку SNMP-параметров контроллеров Sigur.

Для этого необходимо нажать кнопку «Настроить IP-устройства».



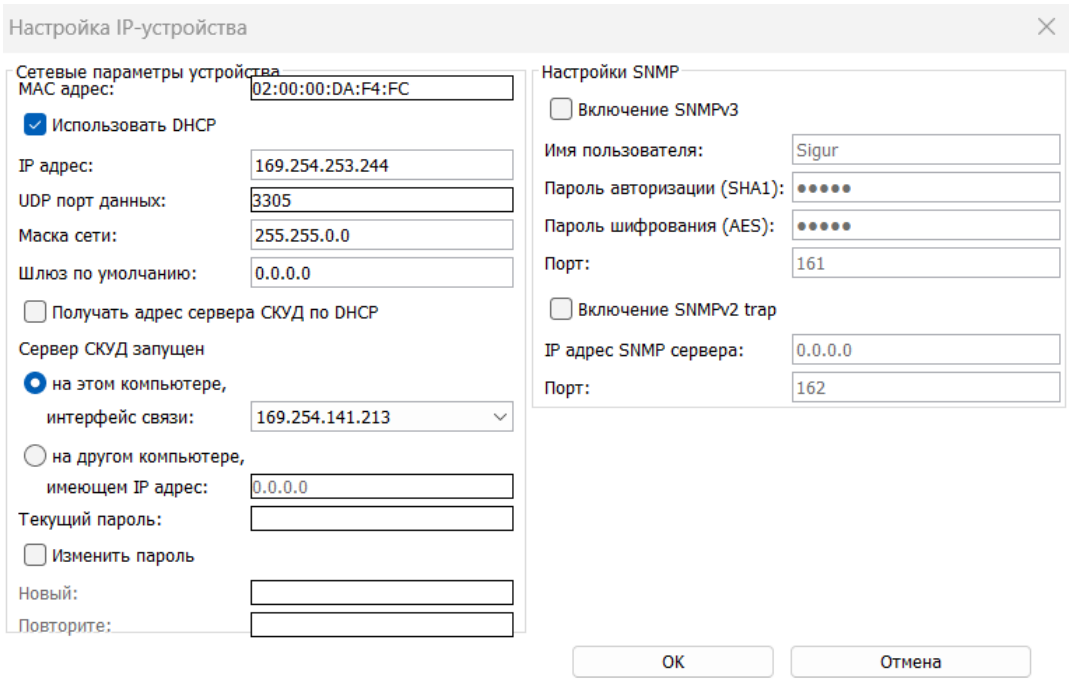
Вкладка «Настройка устройств».

В открывшемся окне выбрать из списка контроллер СКУД, параметры которого необходимо отследить. Нажать на кнопку «Изменить параметры».



Окно настройки IP-устройств.

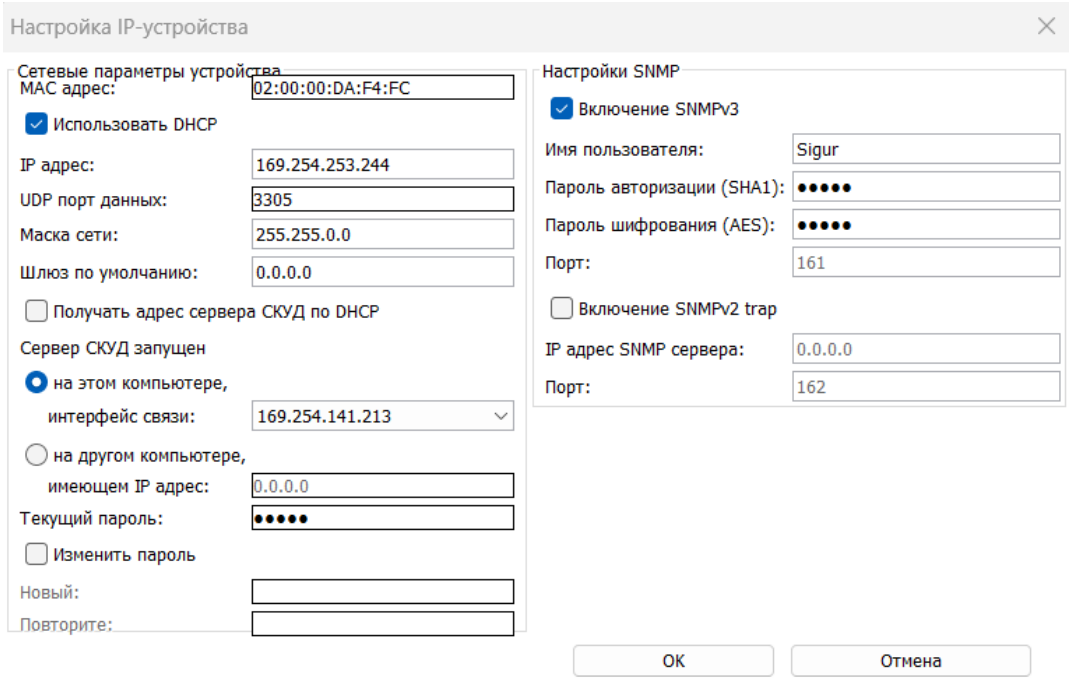
В правой части открывшегося окна необходимо настроить реквизиты подключения внешней системы SNMP к контроллеру.



Окно настройки SNMP.

Включение SNMPv3.

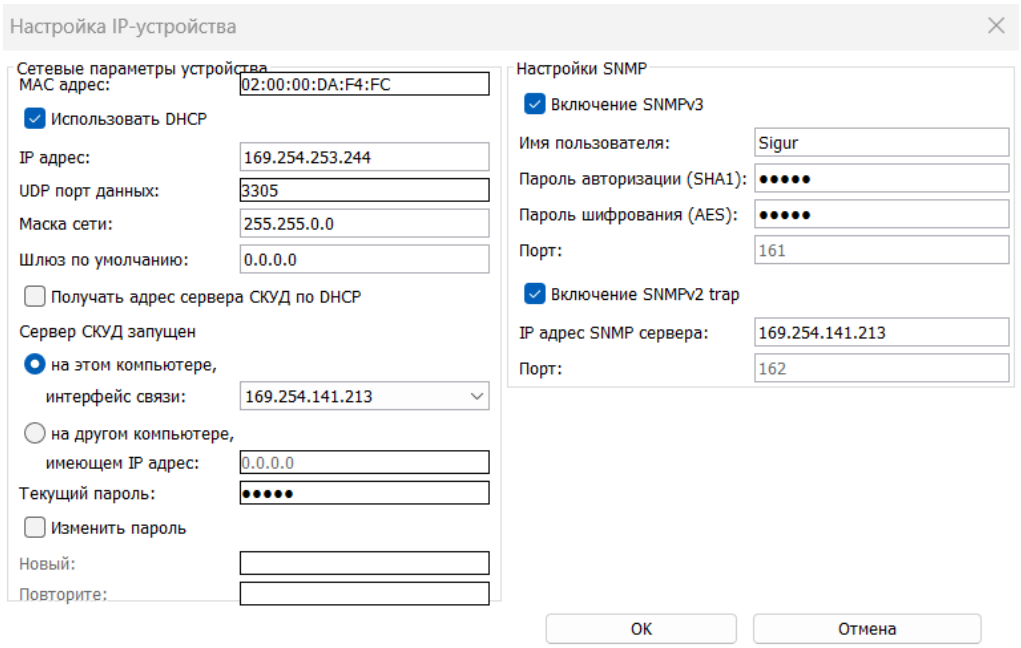
1. Параметр «Имя пользователя» указывает имя, которое будет использоваться для аутентификации при подключении к контроллеру. Значение параметра по умолчанию – **Sigur**, но при необходимости его можно заменить.
2. Параметр «Пароль авторизации (SHA1)» – это пароль, используемый для аутентификации пользователей. Значение параметра по умолчанию – **sigur**, но при необходимости его можно заменить.
3. Параметр «Пароль шифрования (AES)» – это пароль, используемый для шифрования данных, передаваемых между устройствами. Значение параметра по умолчанию – **sigur**, но при необходимости его можно заменить.
4. Параметр «Порт» определяет UDP-порт SNMP-агента (контроллера), на который SNMP-менеджер будет отправлять запрос на получение параметров контроллера. Значение параметра по умолчанию – **161**.



Настройка SNMPv3.

Включение SNMPv2 trap.

1. Задать IP-адрес SNMP сервера, с которым будет осуществляться взаимодействие.
2. Параметр «Порт» определяет UDP-порт SNMP-менеджера, на который SNMP-агент (контроллер) будет отправлять trap-сообщения. Значение параметра по умолчанию – **162**.



Настройка SNMPv2.

После завершения настройки SNMP, в левой части окна необходимо ввести Текущий пароль (по умолчанию – **sigur**), нажать кнопку «OK».

16.1.2. Настройка системы Zabbix

Загрузка MIB-файла и шаблона Sigur.

MIB-файл и шаблон Sigur для настройки параметров для мониторинга в Zabbix можно скачать с сайта Sigur на странице «Главная / Скачать дистрибутивы» в разделе «Прочее».

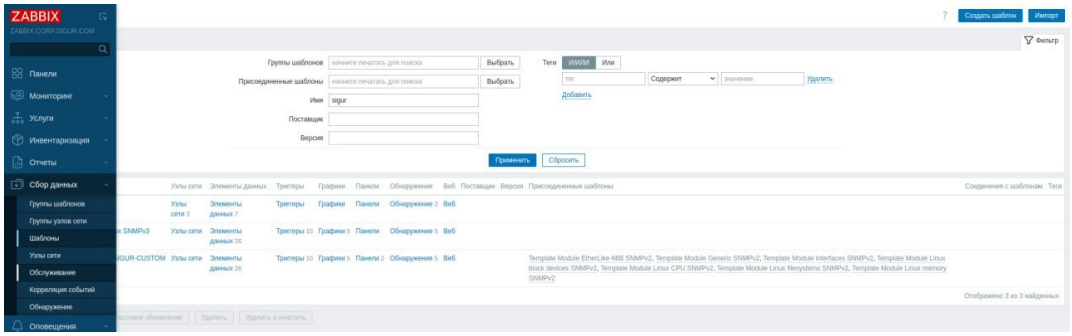
Загрузка MIB-файла.

Перед началом работы необходимо установить и подключить MIB файл к Zabbix. Подробная инструкция как это сделать описана в разделе «MIB файлы» Руководства по Zabbix.

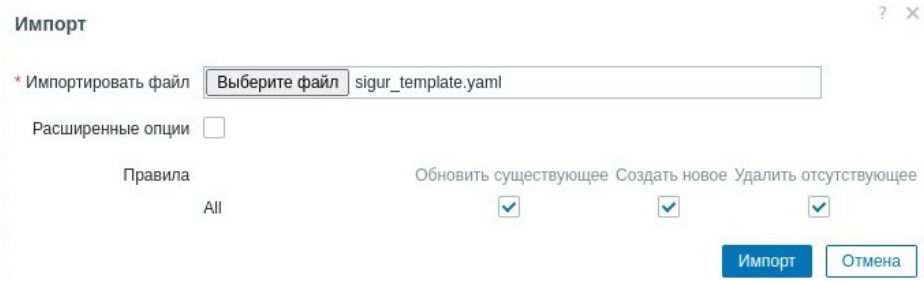
Загрузка шаблона.

Вместо того чтобы настраивать каждое устройство отдельно, можно загрузить шаблон Sigur, который определяет, какие метрики и параметры необходимо мониторить для каждого типа устройств. Пользовательский шаблон Sigur содержит предварительно сконфигурированные элементы мониторинга, условия триггеров и настройки уведомлений.

Пользовательский шаблон Sigur необходимо импортировать в Zabbix. Для этого в правой части окна программы выберите «Шаблоны» – «Импорт»:

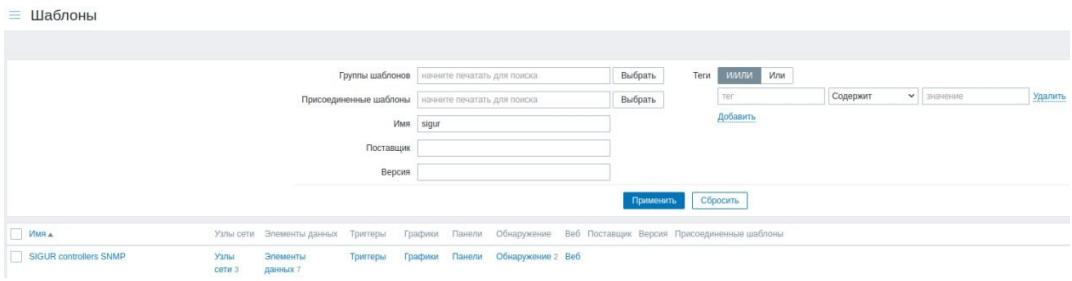


Окно загрузки шаблона Zabbix.



Импорт шаблона.

После этого на вкладке «Шаблоны» появится пользовательский шаблон Sigur:

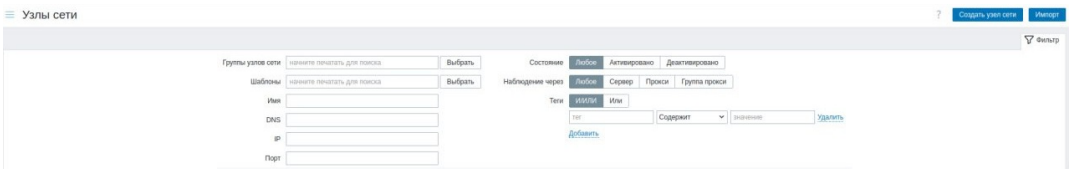


Пользовательский шаблон Sigur.

Далее можно переходить к добавлению узлов сети (контроллеров Sigur).

Добавление узлов сети (контроллеров Sigur).

В левой части окна программы Zabbix выберите вкладку «Узлы сети» и нажмите на кнопку «Создать узел».



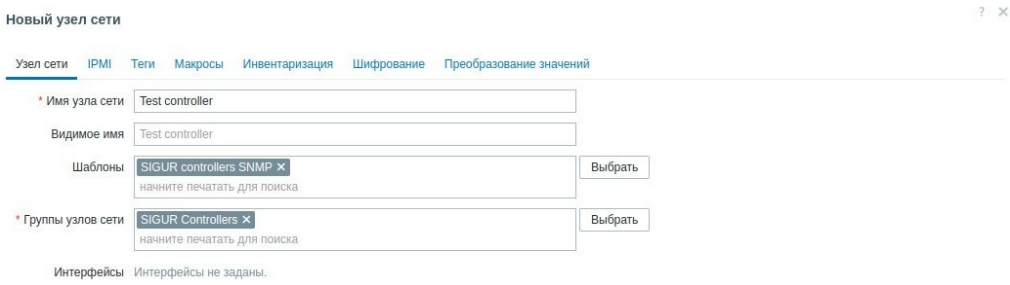
Создание узла сети.

Параметры узла сети.

В появившемся окне необходимо задать основные параметры контроллера:

1. **Имя узла сети** — этот параметр отражает наименование контроллера внутри системы Zabbix.

2. **Видимое имя** — имя узла, отображаемое в окне мониторинга устройств. Задавать данный параметр необязательно.



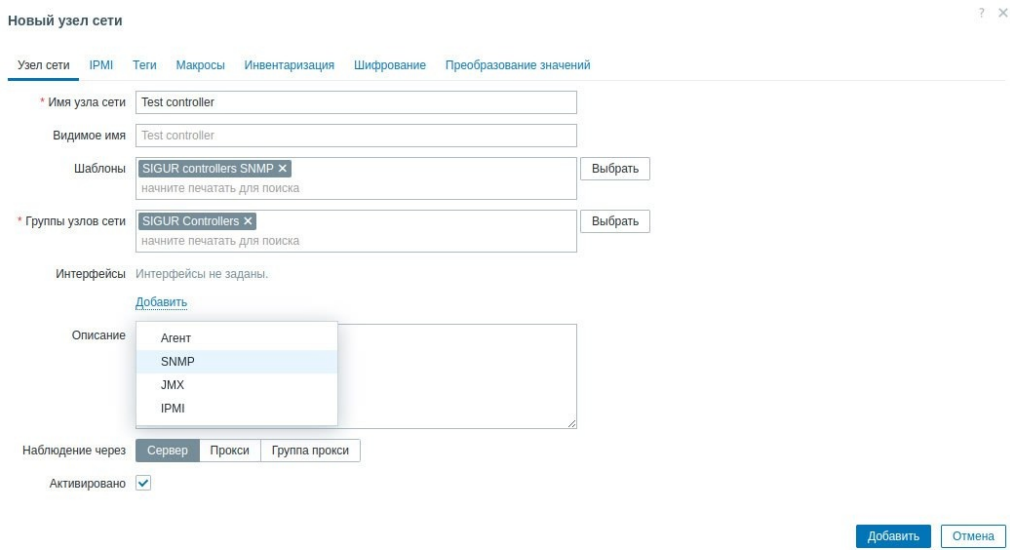
Назначение имени узла сети.

3. **Шаблоны** — пользовательский шаблон, который будет закреплён за этим узлом сети. Здесь необходимо задать предварительно загруженный пользовательский шаблон Sigur:

Выбор пользовательского шаблона для узла сети.

4. **Группы узлов сети** — задаём группу, к которой будет принадлежать контроллер. Все права доступа в Zabbix назначаются на группу узлов сети, а не индивидуально каждому узлу. Поэтому узел сети (контроллер) должен принадлежать хотя бы одной группе.

5. **Интерфейсы** — задаём интерфейс мониторинга состояния узлов сети, в нашем случае — SNMP.

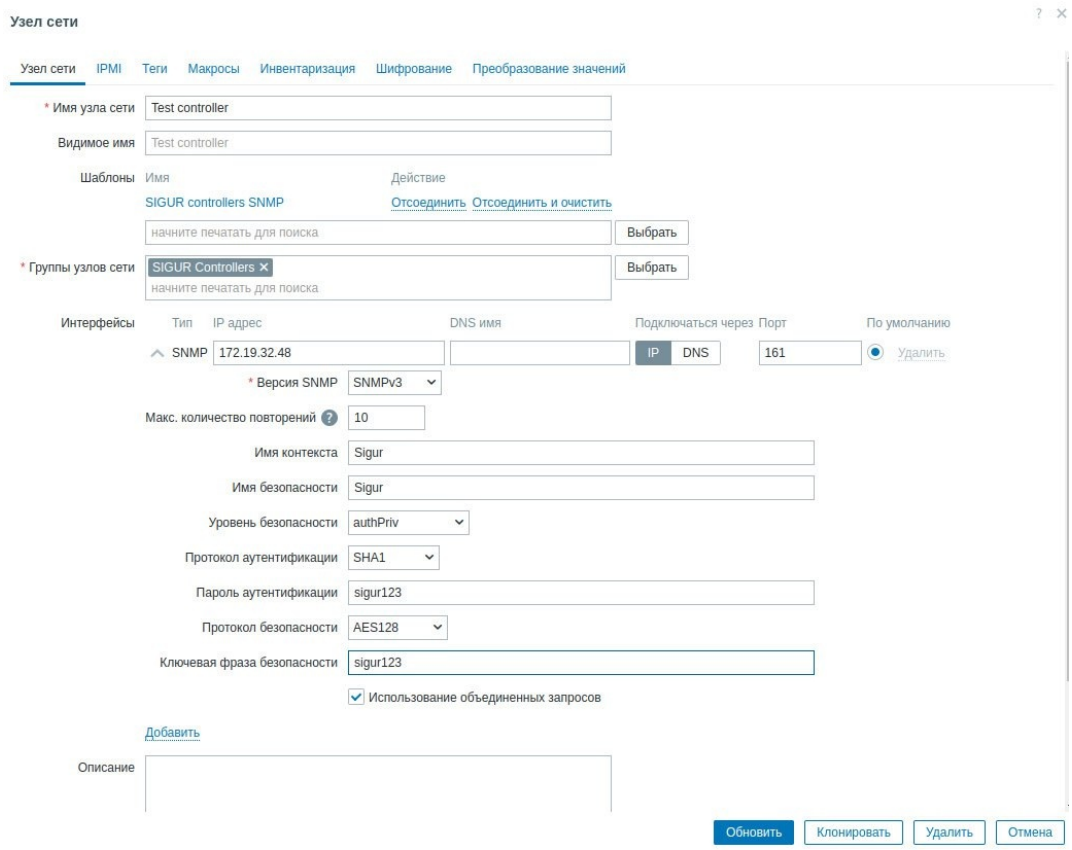


Назначение интерфейса мониторинга.

Далее необходимо задать параметры SNMP:

- IP адрес контроллера;
- Порт – 161 (значение по умолчанию);
- Версия SNMP – SNMPv3;
- Имя контекста – Sigur;
- Имя безопасности – Sigur;
- Протокол аутентификации – SHA1;
- Пароль аутентификации – sigur123;
- Протокол безопасности – AES128;
- Ключевая фраза безопасности – sigur123.

Параметры SNMP в программе Zabbix должны соответствовать параметрам, заданным в ПО «Управление сервером» на вкладке «Настройка IP-устройств».



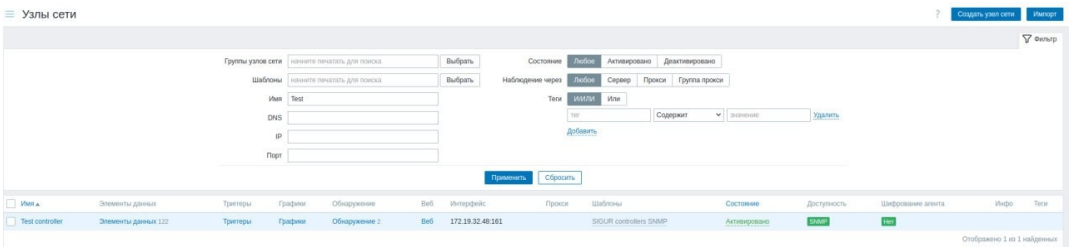
Назначение параметров SNMP в Zabbix.

Настройка узла сети завершена.

Проверка подключения контроллера.

Теперь можно протестировать подключение контроллера СКУД, чтобы убедиться в корректности работы системы мониторинга. В программе Zabbix есть инструменты, которые позволяют проверить связь с устройством и получить информацию о его состоянии.

Для этого перейдите на вкладку«Мониторинг», напишите в поиске имя контроллера и нажмите кнопку «Применить».



Проверка подключения контроллера к системе Zabbix.

В колонке «Состояние» будет указано текущее состояние соединения, а в колонке «Доступность» будет наглядно показано цветом, есть ли связь с устройством по данному протоколу:

- зелёный — связь есть;
- красный — связи нет;
- серый — неизвестно.

16.2. Мониторинг состояния контроллера в программе Zabbix

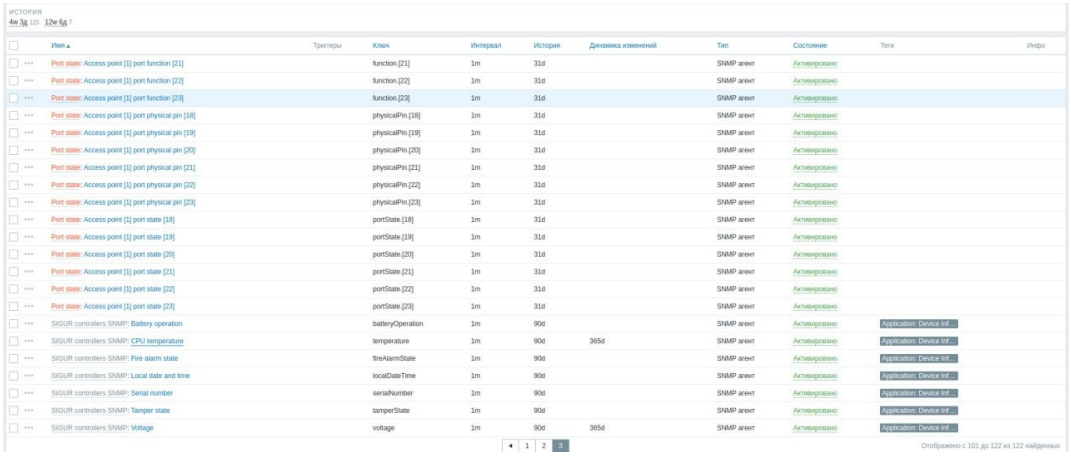
Контроллеры Sigur поддерживают работу с системой мониторинга Zabbix по протоколу SNMP. Процесс мониторинга состояния контроллера системой Zabbix по протоколу SNMP включает следующие шаги:

1. Настройка контроллера в качестве SNMP-агента. Необходимо настроить SNMP-агент, который будет собирать и передавать информацию о своём состоянии в систему мониторинга.
2. Создание SNMP-устройств в Zabbix. В системе мониторинга Zabbix нужно создать новые SNMP-устройства (Узлы сети) для каждого контроллера СКУД. Для этого необходимо указать IP-адрес или имя хоста контроллера, а также другие параметры настройки SNMP.
3. Определение параметров мониторинга. Нужно определить, какие параметры состояния контроллера будут отслеживаться. Эти параметры содержатся в пользовательском MIB-файле.
4. Настойка шаблонов мониторинга. В Zabbix можно использовать шаблоны для настройки мониторинга различных устройств – пользовательский шаблон Sigur.
5. Сбор данных. После настройки SNMP-агентов и параметров мониторинга система Zabbix начнёт собирать данные о состоянии контроллеров СКУД через протокол SNMP. Собранные данные будут храниться в базе данных Zabbix.
6. Уведомления. Zabbix может отправлять уведомления при возникновении определённых событий или условий. Для этого необходимо выполнить настройку триггеров.
7. Визуализация данных. Система мониторинга Zabbix предоставляет различные способы визуализации собранных данных.

16.2.1. Работа в системе мониторинга Zabbix

Работа с элементами данных.

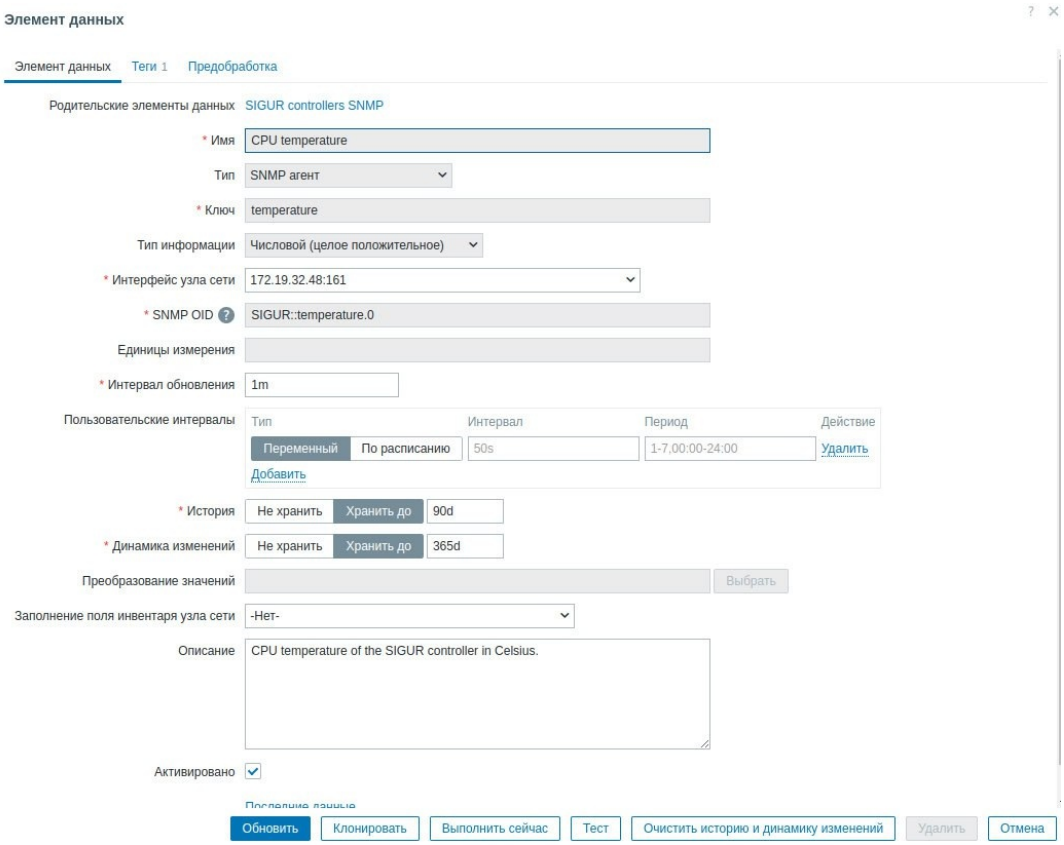
В колонке «Элементы данных» отображается перечень всех параметров, полученных от контроллера:



Перечень параметров контроллера.

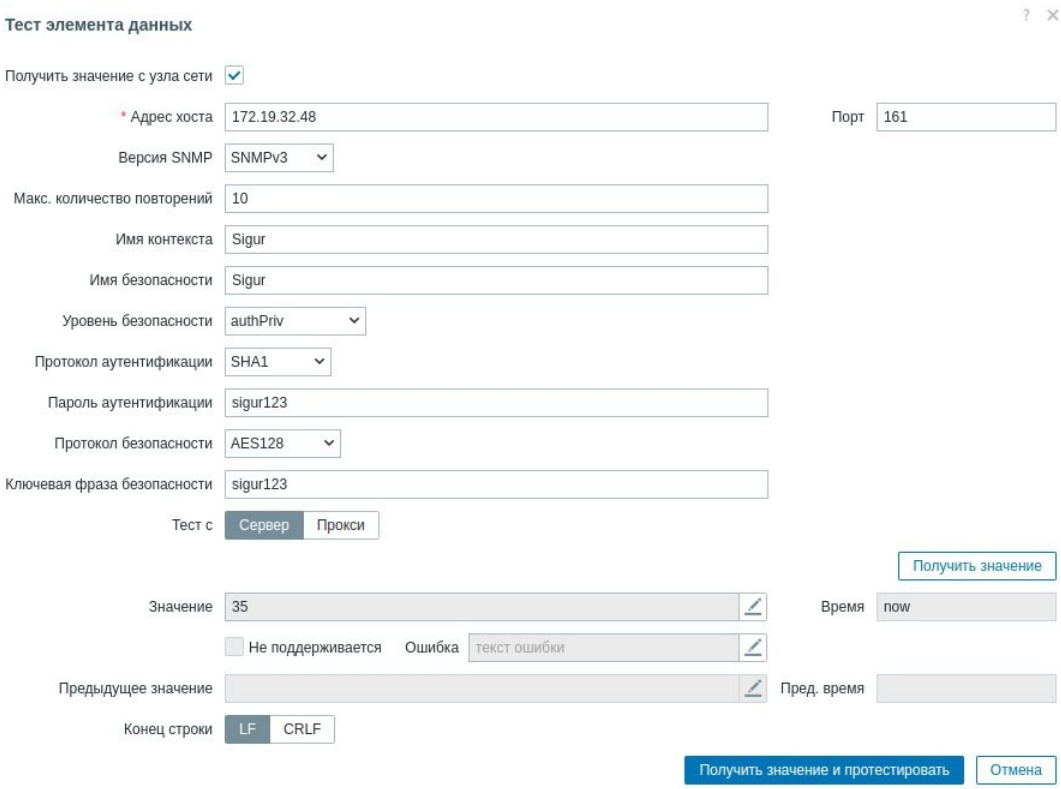
При выборе одного параметра из колонки «Элементы данных» откроется окно с информацией о параметре: тип значения, OID, описание параметра и т. д.

Выберем один из параметров, например CPU temperature (температура контроллера):



Параметр CPU temperature.

Для получения текущего значения выбранного параметра нажмите кнопку «Тест»:



Текущее значение параметра.

Текущее значение параметра CPU temperature (температура контроллера): 35°C.

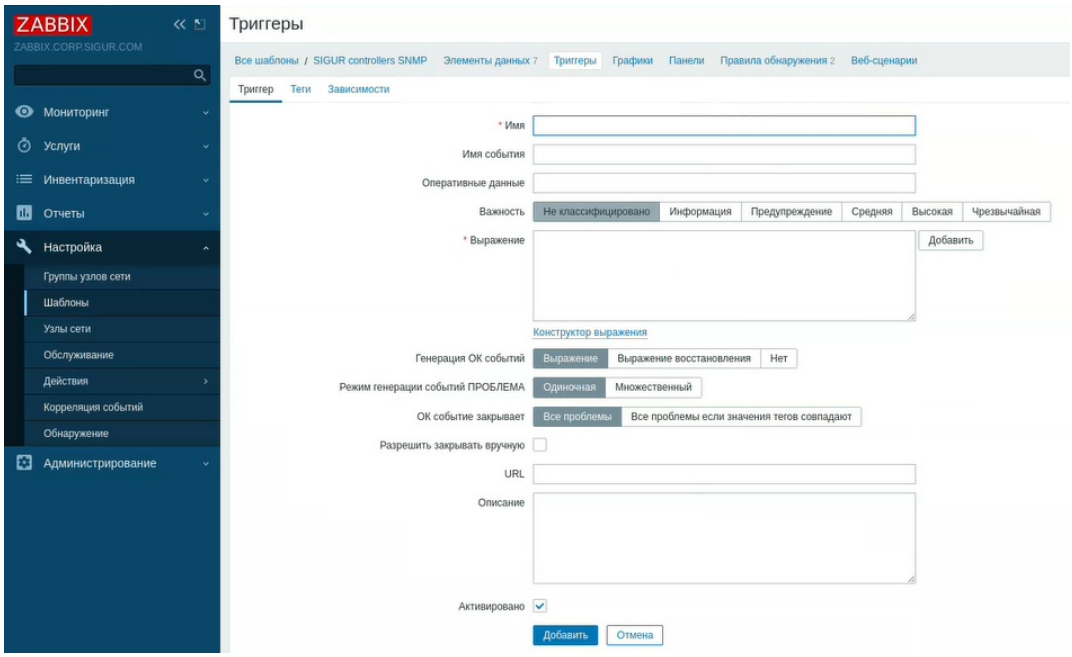
Работа с триггерами.

Система мониторинга Zabbix может отправлять уведомления при возникновении определённых событий или условий. При взаимодействии с контроллерами Sigur триггеры в системе Zabbix могут быть использованы для обнаружения и оповещения о следующих событиях:

- срабатывание шлейфа пожарной сигнализации;
- падение напряжения питания контроллера;
- потеря связи с OSDP считывателем (только контроллеры E2 и E4);
- зафиксированный контроллером факт взлома точки доступа и т. д.

Для этого необходимо создать триггер на сервере Zabbix.

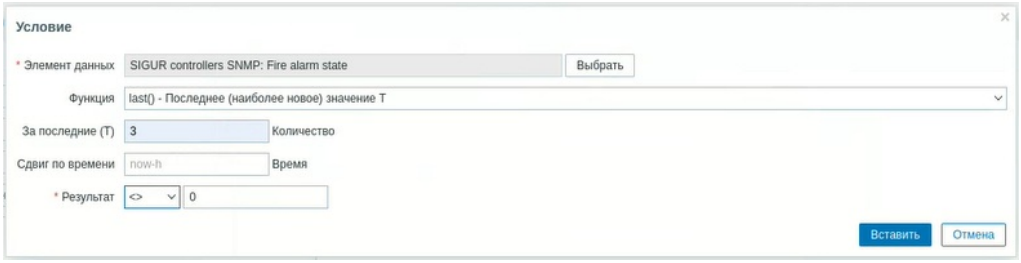
Перейдите на вкладку «Настройка» – «Шаблоны». В открывшемся окне выберите вкладку «Триггеры», нажмите кнопку «Создать триггер».



Окно создания триггера.

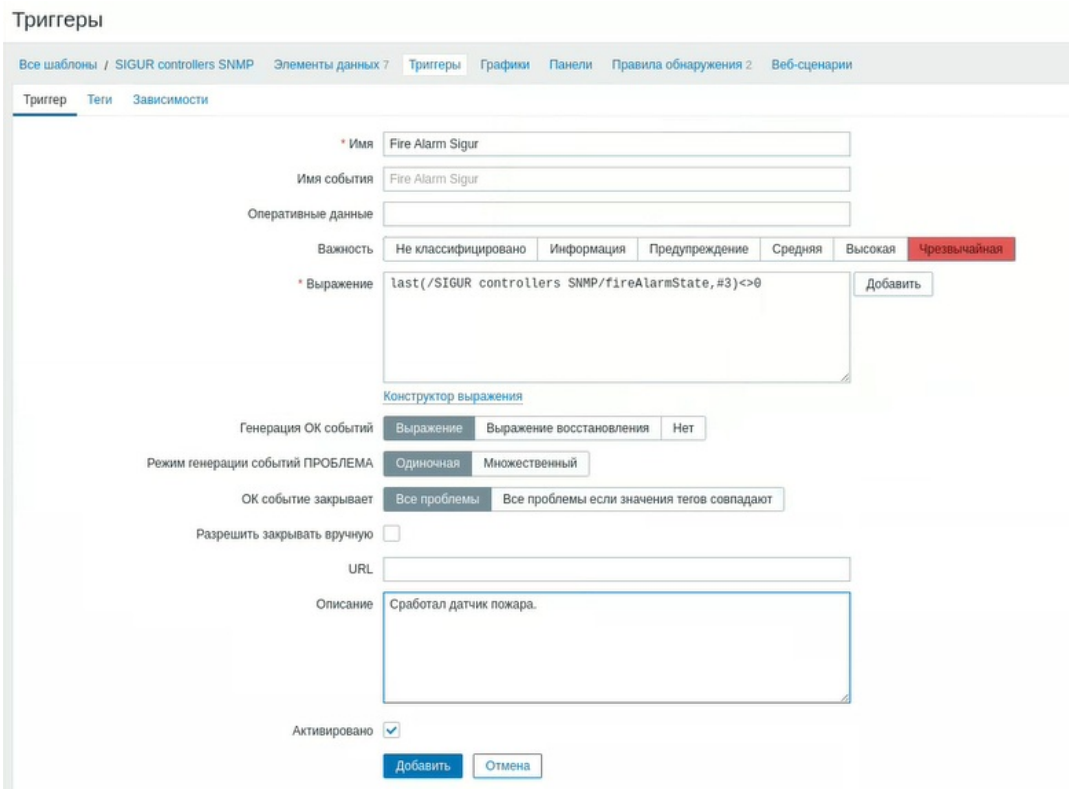
Далее необходимо задать параметры:

1. Имя – системное имя триггера.
2. Имя события – видимое имя, отображаемое в пользовательском интерфейсе.
3. Важность – приоритет реакции системы на триггер.
4. Выражение – определяет, в чём выражается триггер, и как система будет реагировать на него.



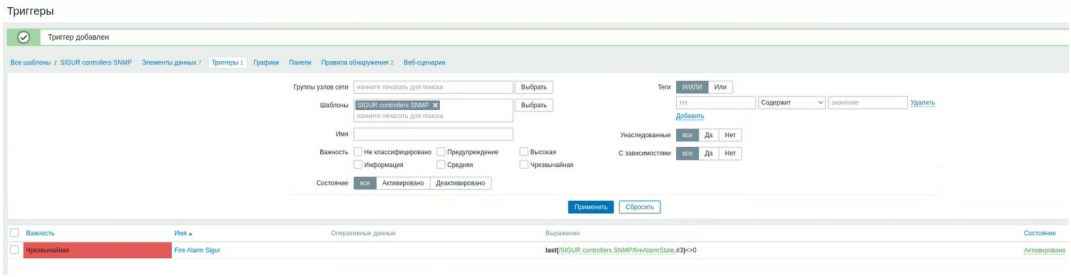
Пример выражения триггера Fire alarm state.

5. Описание – описание триггера в системе или уведомления.
6. Активировано – чекбокс для активации триггера.



Пример триггера Fire Alarm Sigur.

Для завершения настроек нажмите кнопку «Добавить». На вкладке «Триггеры» будут отображаться все созданные триггеры.



Вкладка «Триггеры».

17. Управление сервером через командную строку (AdminCLI)

17.1. Описание инструмента

AdminCLI – это инструмент для управления сервером Sigur через командную строку, подходящий для Linux-систем без графического интерфейса. Он позволяет выполнять различные задачи по администрированию сервера и базы данных Sigur подобно графической утилите «Управление сервером».

С помощью AdminCLI возможно:

- Остановить и запустить серверный модуль, проверить его статус.
- Установить тип базы данных, указать реквизиты подключения к внешней БД и протестировать его, выполнить сброс и обновление БД. Задать названия БД и названия схем БД в случае PostgreSQL.
- Настроить порты незащищённого и безопасного подключения, порты интеграций.
- Установить хранилище сертификатов сервера для подключения по TLS, включить взаимную аутентификацию (mTLS), настроить использование списка отозванных сертификатов и активировать перенаправление запросов к БД через сервер.
- Загрузить JSON-файл ролевой модели и получить информацию о нём.
- Отправить заявку на подключение к центральному серверу и проверить её статус, а также отключиться от центрального сервера.

17.2. Разделы интерфейса

Утилита AdminCLI содержит несколько разделов, перечисленных ниже. Вы также можете перемещаться между разделами в интерактивном режиме, выполняя команды для изменения серверных параметров.

Основные команды.

Команда	Описание	Пример использования
help	Вызов справки и отображение текущих значений параметров. Доступно из любого раздела.	*spnxcli help* *spnxcli service help* *spnxcli database help* *spnxcli security help* *spnxcli ports help*

Команда	Описание	Пример использования
spnxcli	Переход в интерактивный режим. Чтобы переместиться в раздел, введите его название и нажмите Enter. Для навигации между разделами утилиты можно использовать команды: • back – переход в раздел выше уровнем (предыдущий). • exit – выход из корневого раздела (выход из интерфейса и его остановка). • Ctrl+C – закрытие утилиты.	*spnxcli*

17.2.1. Service

Раздел аналогичен вкладке «Состояние» ПО «Управление сервером».

Команды раздела Service.

Команда	Описание	Пример использования
status	Отображение статуса серверного модуля СКУД.	*spnxcli service status*
restStatus	Отображение статуса веб-сервисов.	*spnxcli service restStatus*
startSphinxd	Запуск серверного модуля.	*spnxcli service startSphinxd*
stopSphinxd	Остановка серверного модуля.	*spnxcli service stopSphinxd*

17.2.2. Database

Раздел аналогичен вкладке «База данных» ПО «Управление сервером».

Команды раздела Database.

Команда	Описание	Пример использования
setType {VALUE}	Установка типа используемой базы данных. Возможные значения: • **mysql** – внешняя MariaDB. • **postgres** – внешняя PostgreSQL.	*spnxcli database setType mysql*
setHost {VALUE}	Установка хоста подключения к БД.	*spnxcli database setHost 127.0.0.1*
setPort {VALUE}	Установка порта подключения к БД.	*spnxcli database setPort 3306*
setLogin {VALUE}	Установка логина пользователя БД.	*spnxcli database setLogin user*
setPassword {VALUE}	Установка пароля для подключения к БД.	*spnxcli database setPassword 123456*
setDatabase {VALUE}	Установка имени БД сервера (в случае использования PostgreSQL).	*spnxcli database setdatabase sigur_db*
setSchema {VALUE}	Установка имени схемы БД сервера (в случае использования PostgreSQL). По умолчанию используется схема public.	*spnxcli database setSchema sigur*

Команда	Описание	Пример использования
ChangeServiceDbName {service_name} {new DB name}	Установка имён БД веб-сервисов (в случае использования PostgreSQL). По умолчанию используются имена auth, events, notification, visitrequest, sync.	*spnxcli database ChangeServiceDbName auth-service AuthDB*
ChangeServiceDbSchema {service_name} {new DB schema}	Установка имён схем БД веб-сервисов (в случае использования PostgreSQL). По умолчанию используется схема public.	*spnxcli database ChangeServiceDbSchema auth-service sigur*
test	Тест подключения к БД*.	*spnxcli database test*
reset	Сброс и инициализация БД.	*spnxcli database reset*
init	Инициализация БД. Используется вместо reset, если у пользователя БД нет прав на удаление/создание БД.	*spnxcli database init*
update	Обновление версии формата БД. При выполнении команды без аргументов запрашивается логин и пароль пользователя БД. В случае использования команды с одним аргументом (логин), запрашивается только пароль.	*spnxcli database update* *spnxcli database update user*

* Значение Current database version:[-1], полученное при тестировании подключения к PostgreSQL, означает, что БД создана, но не проинициализирована. Требуется выполнить сброс/инициализацию БД.

17.2.3. Ports

Раздел аналогичен вкладке «Порты» ПО «Управление сервером».

Команды раздела Ports.

Команда	Описание	Пример использования
set {PORT_GROUP} {VALUE}	Включение или отключение группы портов. Доступные значения параметра {PORT_GROUP}: • **ClientGroup** – порты незащищённого подключения к серверу Sigur. • **ClientSecureGroup** – порты защищённого подключения к серверу Sigur. • **Integrations** – порты интеграций (OIF). • **RestApi** – порт REST API. Доступные значения {VALUE}: • **FALSE** – отключить группу портов. • **TRUE** – включить группу портов.	*spnxcli ports set ClientGroup TRUE*
setDefaultPort {TYPE} {VALUE}	Настройка незащищённых портов подключения. Доступные значения параметра {TYPE}: • **Gate {VALUE}** – порт клиентских подключений. • **DBProxy {VALUE}** – порт доступа БД. • **Fg {VALUE}** – порт доступа к видеоархиву СКУД.	*spnxcli ports setDefaultPort Gate 3308*

Команда	Описание	Пример использования
setTlsPort {TYPE} {VALUE}	Настройка портов безопасного подключения. Доступные значения параметра {TYPE}: • **Gate {VALUE}** – порт клиентских подключений. • **DBProxy {VALUE}** – порт доступа БД. • **Fg {VALUE}** – порт доступа к видеоархиву СКУД.	*spnxcli ports setTlsPort Gate 3309*
setIntegrationPort OIF {VALUE}	Настройка порта для подключения по OIF.	*spnxcli ports setIntegrationPort OIF 3312*
setEnableOifTls {VALUE}	Настройка TLS на порте интеграции OIF. Доступные значения: • **FALSE** – не использовать TLS. • **TRUE** – использовать TLS.	*spnxcli ports setEnableOifTls TRUE*
setRestApiPort Gateway {VALUE}	Настройка порта REST API.	*spnxcli ports setRestApiPort Gateway 9500*
setEnableRestApiTls {VALUE}	Настройка TLS на порте REST API. Доступные значения: • **FALSE** – не использовать TLS. • **TRUE** – использовать TLS.	*spnxcli ports setEnableRestApiTls TRUE*

17.2.4. Security

Раздел аналогичен вкладке «Безопасность» ПО «Управление сервером».

Команды раздела Security.

Команда	Описание	Пример использования
setStore {VALUE}	Установка хранилища сертификатов сервера СКУД. Доступные значения: • **NOT_USED** – хранилище сертификатов сервера не используется. • **PKCS12 {STORE_PATH} {PASSWORD}** – используется хранилище типа PKCS#12. Необходимо передать путь {STORE_PATH} и пароль {PASSWORD} к хранилищу формата *.p12.	*spnxcli security setStore PKCS12 /opt/acs_server.p12 123456*
setMutualAuth {VALUE}	Настройка взаимной аутентификации. Если взаимная аутентификация включена, то сервер СКУД будет требовать сертификат клиентов, подключающихся по TLS. Доступно, если задано хранилище сертификатов сервера СКУД. Возможные значения: • **FALSE** – выключить. • **TRUE** – включить.	*spnxcli security setMutualAuth TRUE*
setMutualAuthRest {VALUE}	Использование взаимной аутентификации REST API. Если включено, то при использовании REST API будут требоваться сертификаты клиентов, подключающихся по TLS. Возможные значения: • **FALSE** – выключить. • **TRUE** – включить.	*spnxcli security setMutualAuthRest TRUE*

Команда	Описание	Пример использования
setEnableCrl {VALUE}	Использование списка отозванных сертификатов. Доступно, если включена взаимная аутентификация. Возможные значения: • **FALSE** – выключить. • **TRUE {STORE_FORMAT} {STORE_PATH}** – включить. Необходимо передать расширение файла {STORE_FORMAT} и путь {STORE_PATH} к хранилищу отозванных сертификатов. Расширение может принимать значения PEM или DER.	*spnxcli security setEnableCrl TRUE PEM /opt/CRL.pem*
setDBProxy {VALUE}	Перенаправление запросов к БД через сервер СКУД. Доступные значения: • **FALSE** – выключить. • **TRUE** – включить.	*spnxcli security setDBProxy TRUE*

17.2.5. Roles

Команды раздела Roles.

Команда	Описание	Пример использования
upload {VALUE}	Загрузка JSON-файла ролевой модели.	*spnxcli roles upload /home/User/Downloads/roles.json*
info	Отображение информации о ролевой модели.	*spnxcli roles info*

17.2.6. CentralServer

Раздел аналогичен вкладке «Подключение к центральному серверу» ПО «Управление сервером».

Команды раздела CentralServer.

Команда	Описание	Пример использования
status	Отображение статуса заявки на подключение к центральному серверу.	*spnxcli CentralServer status*
disconnect	Отключение от центрального сервера.	*spnxcli CentralServer disconnect*
connect [name] [key_connection] [ip_or_domain] [port]	Подключение к центральному серверу.	*spnxcli CentralServer connect NizhnyNovgorod 093708 172.19.5.141 9701*

17.3. Возможные сообщения об ошибках

Сообщение об ошибке	Пояснение
error:Unsupported command	Используется некорректная команда.
error:Unsupported value	Указано некорректное значение параметра в команде.
error:Duplicate port	Указан номер порта, который уже присвоен другому параметру во включённой группе портов.
error:Keystore password was incorrect	Указан неверный пароль к хранилищу сертификатов PKCS#12.
error:The specified file is not an X.509 certificate revocation list	Указан путь к некорректному файлу хранилища отозванных сертификатов.
error:The chain of trust of the key store of the ACS server does not contain X.509 certification authorities	Цепочка доверия в хранилище сертификатов сервера не содержит центр сертификации. Возможные причины: • Используется список отозванных сертификатов от другого центра сертификации. • В сертификате сервера отсутствуют атрибуты для проверки принадлежности списка отозванных сертификатов к тому же центру сертификации, что и сертификат сервера.

18. 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	3309	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 контроллера в режим шифрования данных при взаимодействии с сервером.
3307	Для информационного обмена с контроллерами с шифрованием трафика (DTLS)*.
161	Для информационного обмена с контроллером по протоколу SNMPv3*.
162	Для отправки контроллером Trap-сообщений по SNMPv2*.

* Чтобы уточнить, поддерживает ли конкретная модель контроллера DTLS и SNMP, обратитесь к его руководству по эксплуатации.

19. 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