Система контроля и управления доступом «Sigur».

Руководство администратора.

«Промавтоматика», г. Н. Новгород, 2022 г.

Оглавление:

1. Введение

Данный документ содержит общие сведения о системе Sigur, инструкцию установке и удалению программного обеспечения системы контроля и управления доступом «Sigur», а также инструкцию по эксплуатации программы управления сервером системы.
Предприятие-изготовитель несёт ответственность за точность предоставляемой документации и при существенных модификациях в программном обеспечении обязуется предоставлять обновлённую редакцию данной документации.
Данный документ соответствует версии ПО 1.1.1.30.
Последнюю версию данного документа всегда можно найти на странице https://sigur.com/docs/

2. Используемые определения, обозначения и сокращения

СКУД	Система контроля и управления доступом. Программно–аппаратный комплекс, предназначенный для осуществления функций контроля и управления доступом.
ПО	Программное обеспечение.
БД	База данных.
ПК	Персональный компьютер.

3. Основные принципы работы системы «Sigur»

3.1. Обзор компонентов

СКУД «Sigur» состоит из следующих компонентов:

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

- Контрольный считыватель – используется для оперативного поиска сотрудников в базе данных системы и для быстрого ввода кода нового пропуска в систему. На момент написания документации в качестве контрольных поддерживаются следующие модели: Sigur-Reader-EH (для карт форматов EM Marine и HID ProxCard II), считыватель ACR1252U (для карт Mifare) и подключение любых считывателей с выходным интерфейсом Wiegand-26 к адаптеру Sigur-Reader-W (для прочих форматов карт). Так же для заведения биометрических шаблонов поддерживаются следующие модели: BioSmart FS-80 (FPS-150 – с ограничениями, возможность работы под разными ОС уточняйте у производителя), BioSmart DCR-PV, Anviz U-Bio, ВЗОР-Enroll.
- IP-камеры – (опционально) подразумевается установка камер около исполнительных устройств. По IP-сети могут быть подведены к серверу Sigur для цели трансляции живого видео около исполнительных устройств, а так же накопления фото-архива по факту происходящих на исполнительных устройствах событий, фиксируемых на сервере СКУД. Альтернативно может быть настроена интеграция с серверами систем видеонаблюдения.
- Некоторая компьютерная периферия, (опционально) подключаемая к клиентскому месту системы:
    - web-камеры — для целей оперативного занесения фотографий объектов доступа;
    - сканеры — для цели сканирования изображений и дополнительного закрепления их к объектам доступа; для цели распознавания персональной информации при выдаче пропуска посетителю (требуется отдельное лицензирование);
    - принтеры — для целей печати информации в результате работы некоторых дополнительных функций ПО Sigur.

3.2. Принципы работы системы «Sigur»

3.2.1. Сервер системы

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

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

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

3.2.2. Контроллер системы

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

Независимо от наличия или отсутствия связи с сервером системы, контроллер принимает решение о разрешении/запрете доступа самостоятельно, на основании автономной базы ключей и режимов доступа.

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

Современные схемотехнические решения и алгоритмы программирования позволили добиться следующих результатов:

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

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

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

3.2.3. Связь сервера с контроллерами

В штатном режиме сервер системы опрашивает все подключённые к нему через линии связи RS485 контроллеры, посылая каждому контроллеру запрос о его состоянии, при необходимости передаёт дополнительные данные и получает ответ контроллера. Для IP контроллеров постоянный опрос отсутствует, производится периодический контроль связи путём запроса к контролерам раз в 10 минут.
Работоспособность линий связи сохраняется в широком диапазоне возможных помех за счёт применяемых программных алгоритмов.

3.3. Ключевые элементы базы системы «Sigur»

3.3.1. Список точек доступа СКУД с их настройками

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

3.3.2. 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.
Первый: отделы, в которые возможно вложение других отделов и объектов доступа.
Второй: непосредственно объекты доступа (сотрудники, автомобили, пропуска посетителей).

Каждому элементу списка такого рода присваивается ключ – код пропуска, согласно которому он идентифицируется системой при осуществлении доступа, а также режим, определяющий интервалы разрешения доступа и рабочие графики.
В этом списке так же хранятся пользователи (операторы) системы, настройки их прав доступа к различным функциям СКУД.

3.3.3. Список режимов

Список содержит все режимы, существующие в СКУД. Режимы предназначены для указания правил доступа, интервалов рабочего времени а так же режимов автономной работы ТД.
Режим представляет собой последовательность дней заданной длины (от 1 до 32 дней) с определённой датой начала отсчёта.
В каждом режиме возможно задание дополнительных правил, определяющих логику доступа (требование санкции охраны и пр.)
Существуют четыре вида режимов: уровень 1, уровень 2, уровень 3, уровень 4 (режимы перечислены в порядке усиления приоритета).
Каждому объекту доступа можно присвоить один режим уровня 1 и произвольное количество режимов более высокого уровня (2..4).
Режимы уровней 2, 3 и 4 введены для корректной работы СКУД в ситуациях, когда требуется гибкое временное изменение основного режима. Они имеют приоритет над основным режимом (режимом уровня 1).

3.4. Санкционирование доступа и регистрация событий системы

3.4.1. Принятие решения о санкционировании доступа

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

- Наличие допуска на данную точку доступа.
- Наличие разрешения на допуск в текущее время.
- Наличие разрешения на допуск в нужном направлении.
- Наличие дополнительных проверок для объекта доступа.

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

3.4.2. Регистрация событий системы

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

часами реального времени.
Все зарегистрированные события хранятся в энергонезависимой памяти контроллера и автоматически передаются на сервер СКУД при наличии связи.
Таким образом, в базе данных сервера хранятся все события СКУД, по которым можно получать отчёты за заданные промежутки времени.
Система хранит всю информацию о зарегистрированных ею событиях, начиная с момента её первого запуска, без временных ограничений. Количество событий в системе – неограниченно.

4. Системные требования СКУД «Sigur»

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

4.1. Рекомендуемая конфигурация сервера

- ОС: Windows 10 / Windows Server 2019 / Linux Debian 9 (32-разрядные / 64-разрядные)
- Процессор: уровня Intel Core i7 и выше.
- Память: не менее 8 Гб.
- Свободное место на жёстком диске: 250 Гб.
- 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).

4.2. Минимальная конфигурация сервера

- ОС: не ниже Windows 7 SP1 / Windows Server 2008 R2 SP1 / Linux Debian 8 (32-разрядные / 64-разрядные)
- Процессор: не менее 1 ГГц.
- Память: не менее 2 Гб.
- Свободное место на жёстком диске: 500 Мб 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. Ориентировочный объем, занимаемый данными на жёстком диске – 120 Мб на 1 000 000 произошедших событий.
- Не менее одного свободного USB порта (при наличии HASP-ключа аппаратной защиты).
- Источник бесперебойного питания.
- Разрешение монитора: не менее 1280*1024.
- При работе с большими БД (десятки миллионов проходов и более) – высокоскоростной жёсткий диск (SSD или RAID-массив).

Дополнительные требования при использовании встроенной в Sigur функции распознавания лиц:

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

Примечание: Работа функции распознавания лиц требует уже более заметных мощностей от сервера. В качестве примера: обработка одного кадра на одном ядре Intel Core i5-7260U@2.2GHz занимает порядка 150 мс (т. е. около 26-ти кадров в секунду на 4-х ядерном

процессоре). Однако, данная цифра варьируется в зависимости от размера кадра, модели процессора и многих других параметров.

4.3. Конфигурация клиентского места

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

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

4.4. Требования к операционной системе

Установка сервера и клиентов ПО «Sigur» производится на компьютеры под управлением операционной системы Windows (как 32, так и 64-битной): Windows 7 SP1, Windows Server 2008 R2 SP1 и более новых, а также Linux Debian (как 32, так и 64-битной).
Возможны произвольные комбинации сервера и рабочих мест под управлением разных ОС (например, сервер на Linux, часть клиентов — также на Linux, а другая часть — на Windows).
Независимо от типа используемой операционной системы, необходима установка на неё последних обновлений, выпущенных производителем ОС – компанией Microsoft. Например, для Windows 7 это сервис–пак SP1.

5. Архитектура серверного программного обеспечения

Серверное программное обеспечение состоит из сервера базы данных и серверного модуля системы «Sigur».
Сервер базы данных предоставляет доступ компонентам системы к общей базе данных.
Серверный модуль обеспечивает информационный обмен с контроллерами системы по линии связи.
При установке серверного ПО системы оба компонента сервера регистрируются как службы (сервисы) Windows и запускаются автоматически при загрузке операционной системы.
Для управления компонентами сервера, как правило, используется «Программа управления сервером», описанная в данном руководстве. Также может быть использована стандартная утилита Windows «Службы».
Название служб, используемых системой: "Sphinx database server" и "Sphinx service module".

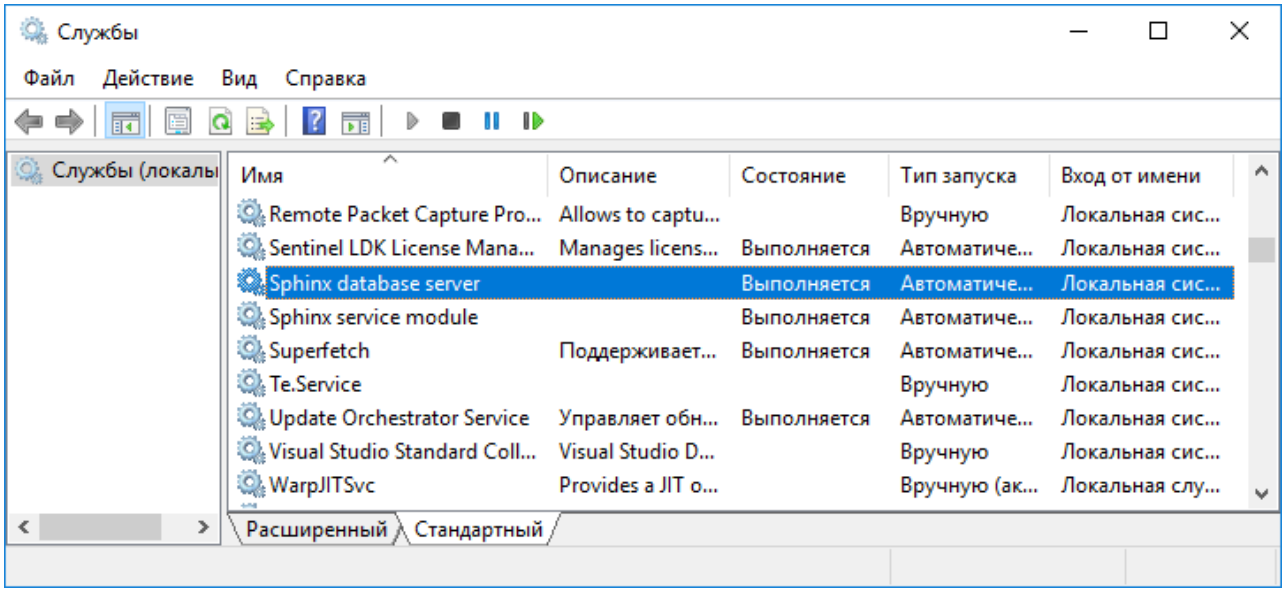


Рис. 1. Управление серверными процессами системы с помощью утилиты «Службы»

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

- "mysqld.exe" являющийся сервером БД.
- "sphinxd.exe" являющийся серверным модулем системы «Sigur».
- "wdt3.exe" являющийся вспомогательной программой, используемой для запуска "sphinxd.exe" и контролирующей его работу.

6. Программное обеспечение системы «Sigur»

Программное обеспечение (ПО) системы «Sigur» построено на основе клиент–серверной архитектуры.
Программное обеспечение сервера состоит из двух программных компонентов. Сервер базы данных (БД) предоставляет доступ всем программным компонентам системы к общей базе данных. Серверный модуль обеспечивает информационный обмен с контроллерами системы по линии связи, а также информационный обмен сервера с клиентскими местами. Для нормальной работы системы оба компонента должны быть запущены. Управление этими модулями осуществляется с помощью программы «Управление сервером СКУД «Sigur».
Программное обеспечение клиентской части состоит из программы «Клиент СКУД «Sigur», которую можно устанавливать на любой компьютер, соединённый с сервером сетью по протоколу TCP. Также возможна установка клиентского ПО непосредственно на сервер СКУД «Sigur».

6.1. Установка системы «Sigur»

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

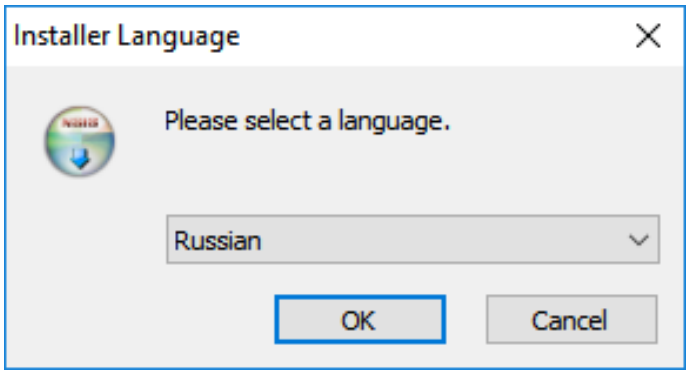


Рис. 2. Выбор языка диалога установки.

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

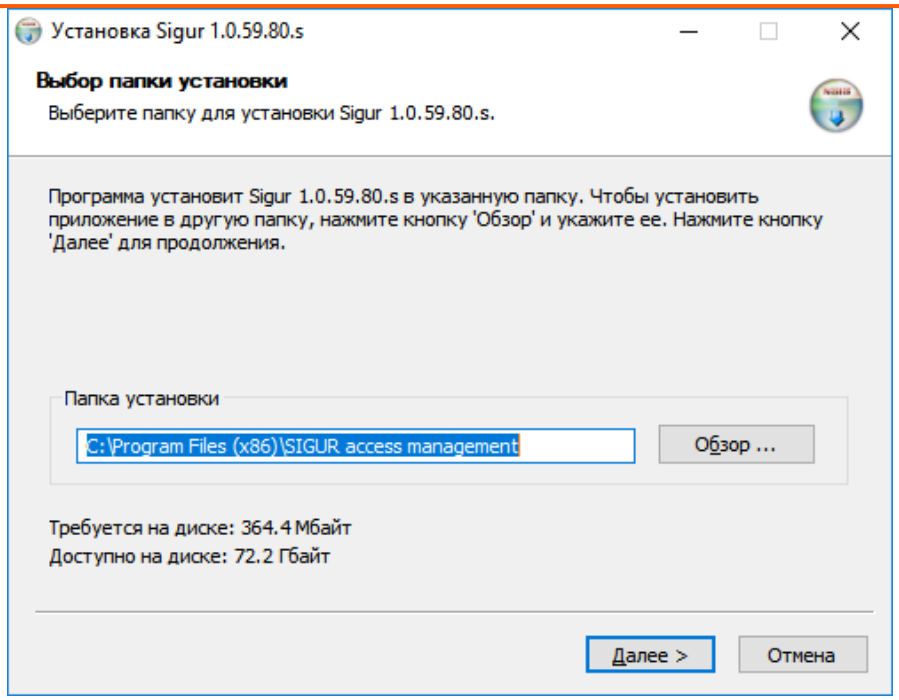


Рис. 3. Выбор папки программы.

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

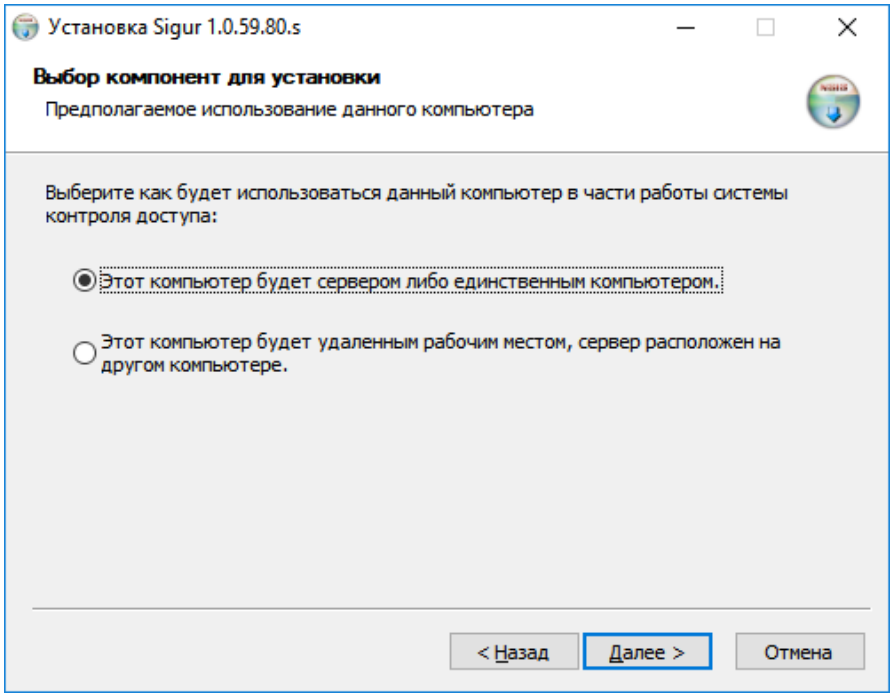


Рис. 4. Выбор типа установки.

После нажатия кнопки «Установить» откроется окно «Копирование файлов», в котором будет отображаться процесс установки программы.

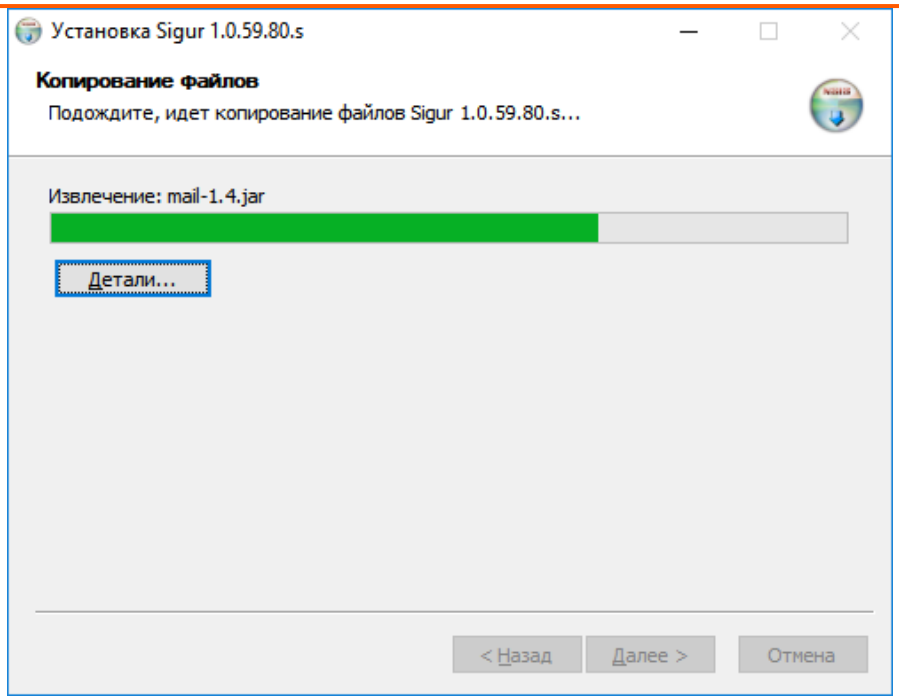


Рис. 5. Процесс установки.

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

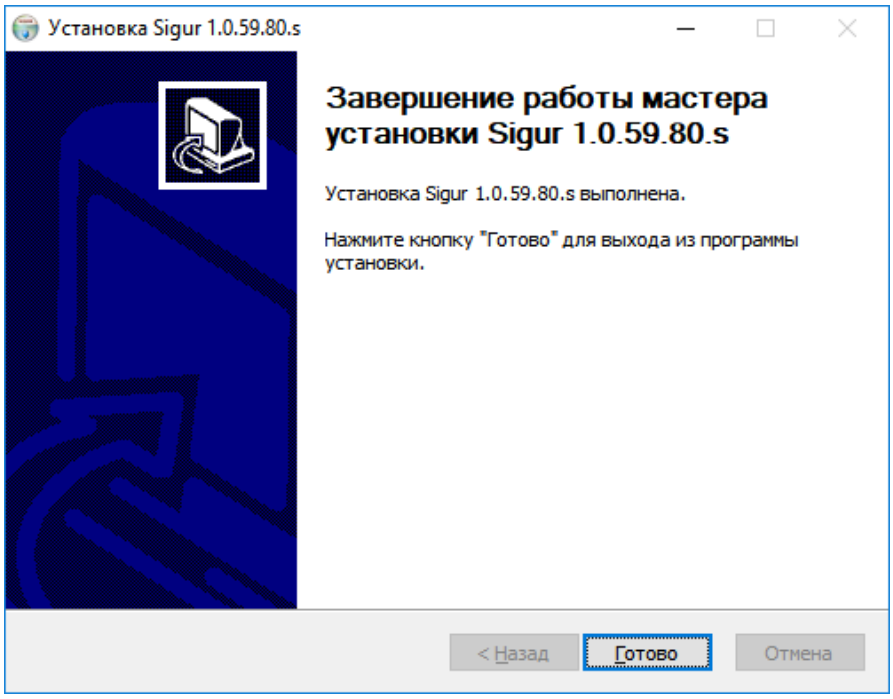


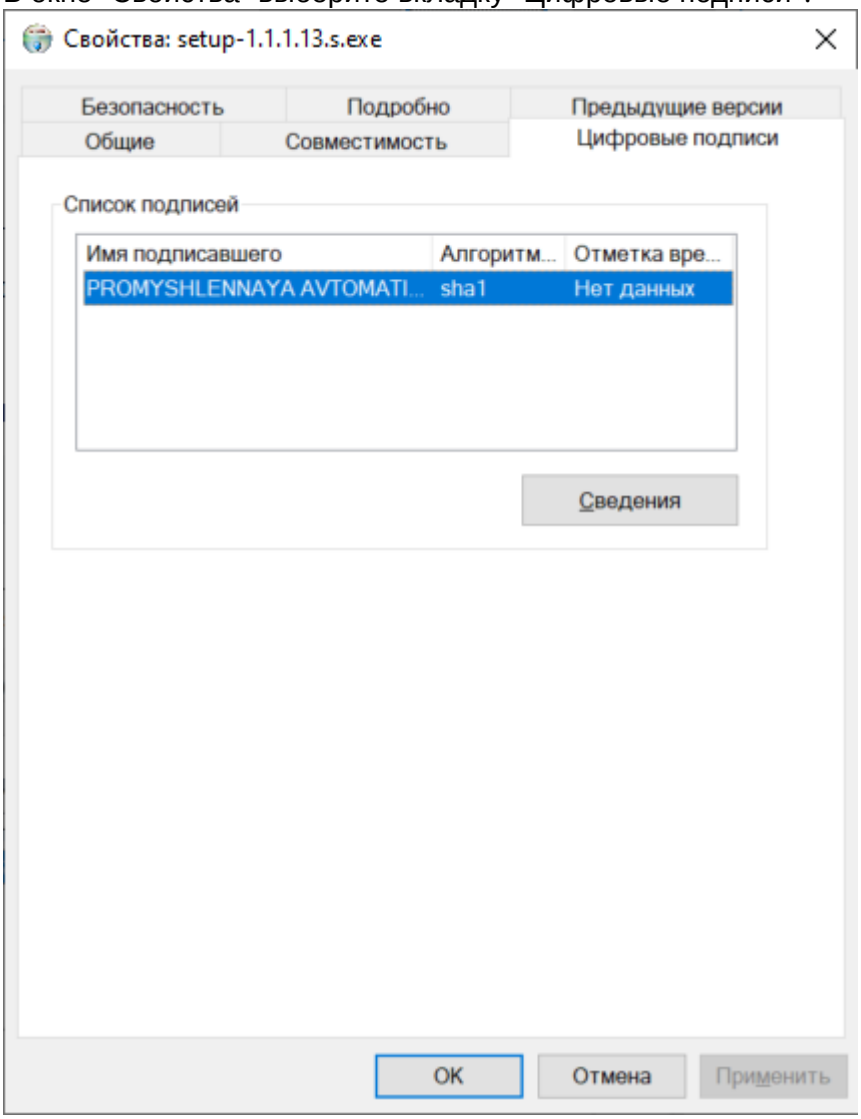
Рис. 6. Завершение работы мастера установки.

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

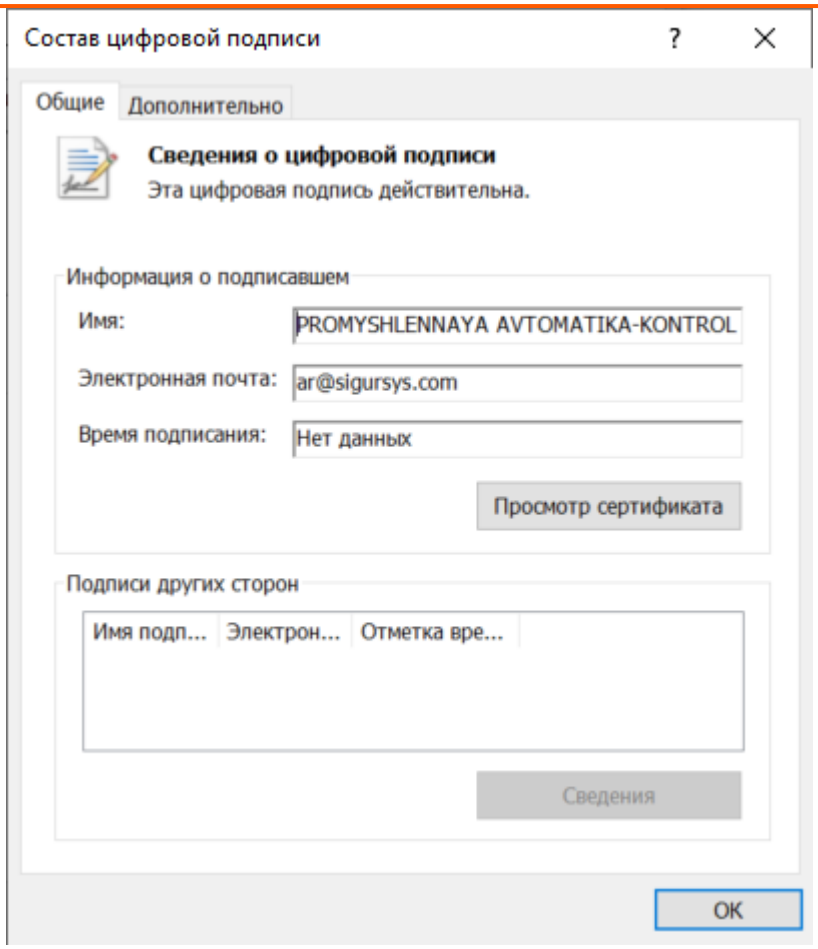
6.1.1. Проверка подлинности (цифровой подписи)

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»:



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



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

6.2. 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», которую можно найти на странице https://sigur.com/docs/

6.3. Удаление системы «Sigur»

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

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

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

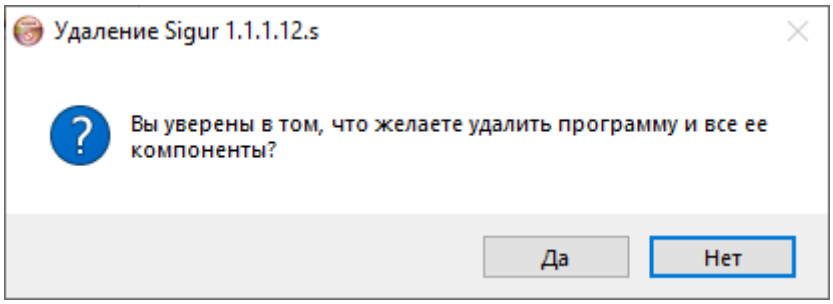


Рис. 7. Запрос удаления программы.

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

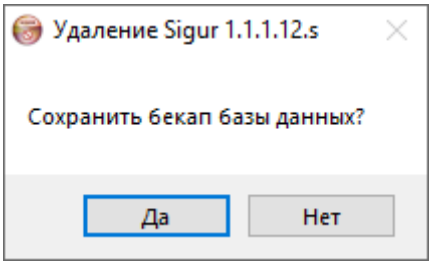


Рис. 8. Запрос сохранения базы данных.

При нажатии кнопки «Да» в каталоге установки ПО будет создан файл с расширением .sql - копия базы данных на этот момент времени. Имя файла будет содержать текущую дату, например “2021-11-21.sql“.

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

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

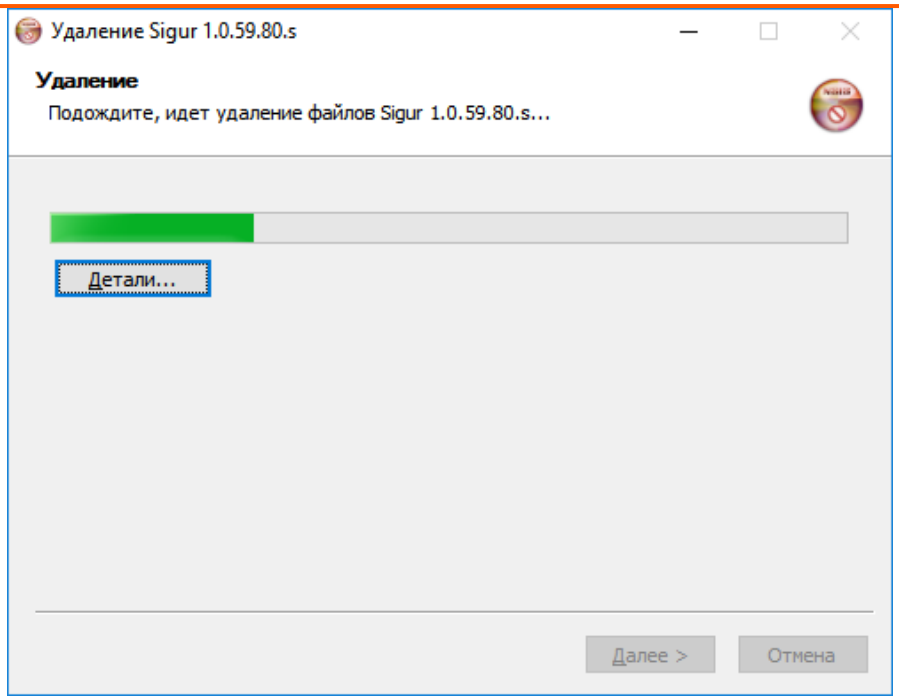


Рис. 9. Процесс удаления программы

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

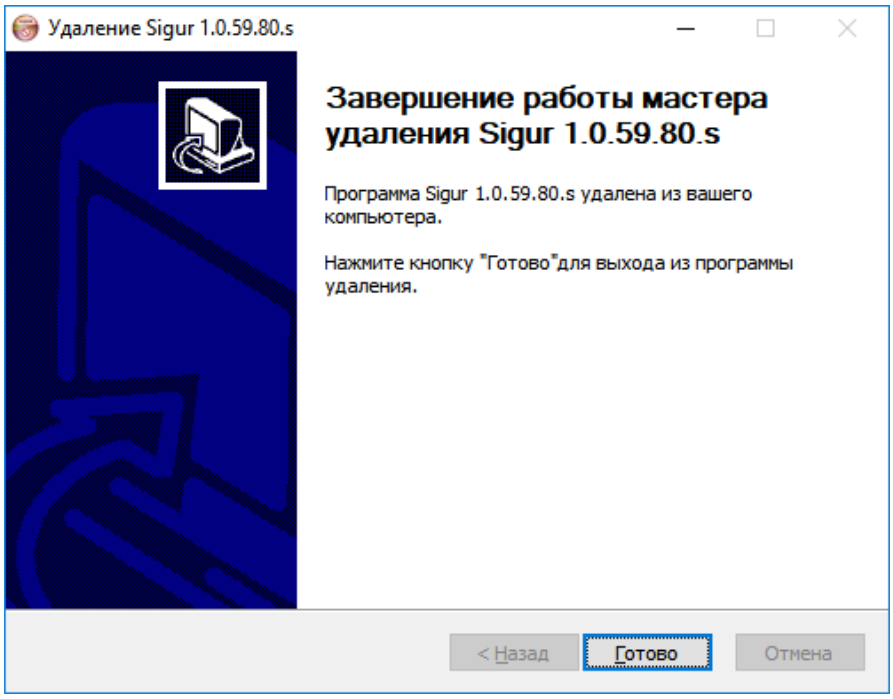


Рис. 10. Завершение работы мастера удаления

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

6.4. Обновление системы «Sigur»

Для обновления сервера, установленного под Windows, необходимо закрыть все графические окна программы и запустить файл setup-XX.exe (где XX – номер версии ПО), аналогичный тому, из которого производилась установка системы. Установщик определит необходимость и возможность обновления автоматически.
По окончании обновления запустите программу управления сервером и нажмите кнопку «Старт» на вкладке «Состояние».
Если при этом потребуется обновление версии базы данных - программа выдаст соответствующий запрос, в ответ на который следует согласиться, нажав кнопку «Да». Никакие данные при этом не будут потеряны.
Клиентские места системы, установленные под Windows, достаточно перезапустить, после чего они обновятся автоматически.
Если в операционной системе настроены политики безопасности, то для автообновления клиентских мест обязателен доступ программы к:

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

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

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

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

6.4.1. Возможные сообщения об ошибках при обновлении ПО

- После запуска установочного файла появляется сообщение “Невозможно открыть файл для записи: “C:\Profram Files (x86)\SIGUR access managment\guinative.dll““:

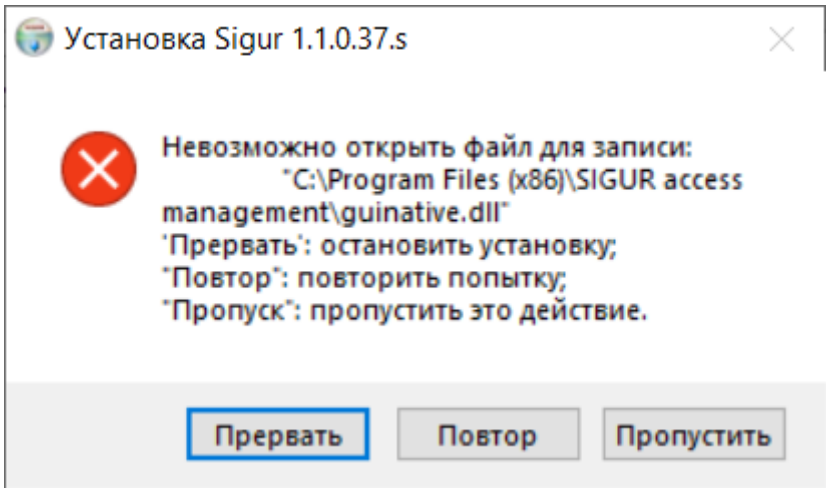


Рис. 11. Пример возможной ошибки в процессе установки

Данная ошибка возникает в том случае, если перед запуском файла установщика не были закрыты все графические окна программы (Управление сервером, Программа управления), 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":

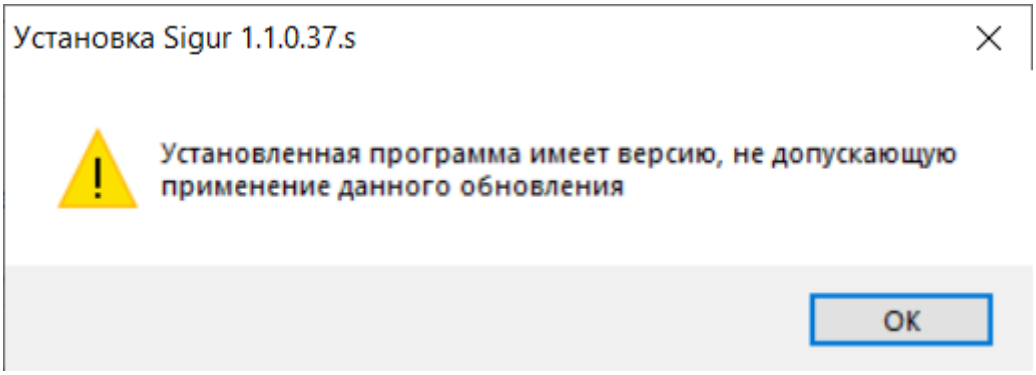


Рис. 12. Пример ошибки при запуске мастера установки

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

6.5. Перенос сервера на другой компьютер

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

- В случае хранения лицензии в памяти HASP-ключа, отключите его от старого сервера и подключите к новому компьютеру. В случае защиты программной лицензией обратитесь к «Руководству пользователя» или в техническую поддержку для привязки лицензии к новому компьютеру.

⚠ **В обязательном порядке выполните сперва перенос лицензии на новый сервер, и только после успешной активации лицензии на новом сервере — переходите к последующему переносу самой базы данных (описанному в пунктах ниже).**

- Запустите программу «Управление сервером СКУД «Sigur».
- 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!
- Установите ПО Sigur на новый компьютер.
- Запустите на новом компьютере с помощью программы «Управление сервером» компонент «Сервер БД». На предложение о создании новой базы данных выберите «нет».
- Произведите импорт БД. Для этого нажмите кнопку «Импорт базы» на закладке «База данных», выберите сохранённый ранее файл и нажмите кнопку «Открыть».
- После завершения импорта текущая версия БД может не совпадать с нужной версией («старая» БД и «новое» ПО), в этом случае нажмите кнопку «Обновить».

- Запустите компонент «Серверный модуль» на вкладке «Состояние».
- В случае использования IP контроллеров (E серия) измените всем им параметр «Подключение», введя IP адрес нового сервера.

6.6. Переход с бесплатной версии ПО на платную

Для перехода с бесплатной версии системы на платную вставьте в сервер HASP ключ аппаратной защиты или загрузите программную лицензию.

7. Программа управления сервером

Программа управления сервером предназначена для наблюдения за состоянием компонентов сервера, настройки резервирования базы данных, добавления в систему новых IP контроллеров и так далее.

7.1. Запуск программы

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

7.2. Главное окно программы

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

Внешний вид главного окна программы:

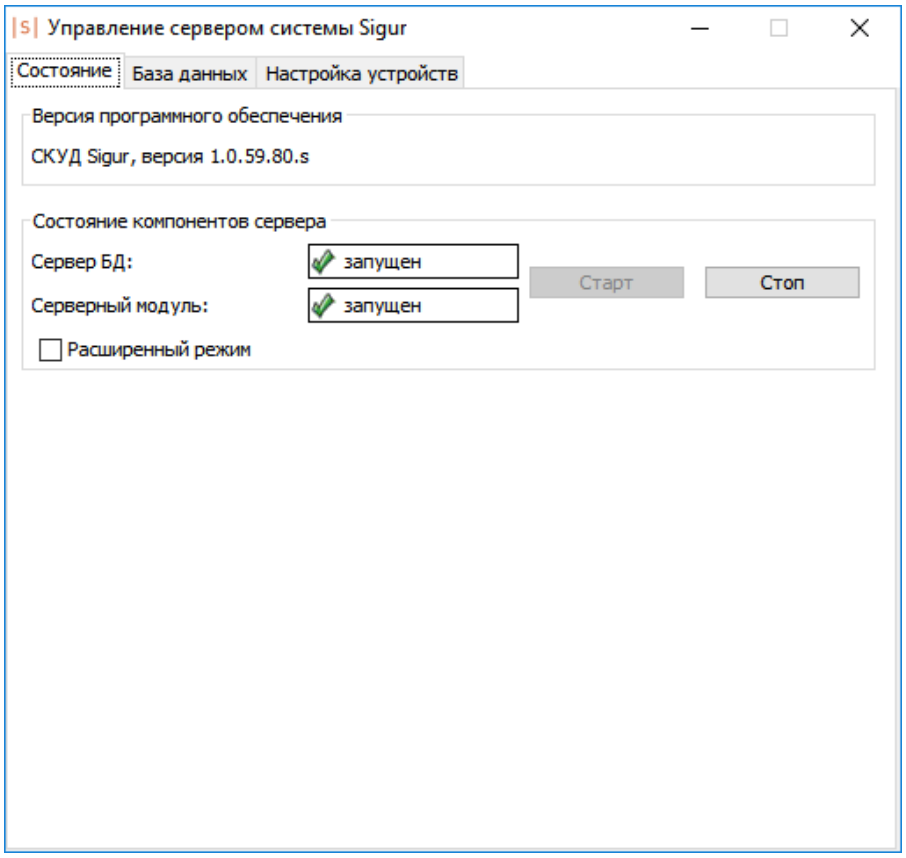


Рис. 13. Окно программы управления сервером, вкладка Состояние

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

Функции управления сервером СКУД распределены по вкладкам: «Состояние», «База данных» и «Настройка устройств».

8. Управление компонентами сервера

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

Обычный режим управления компонентами сервера:

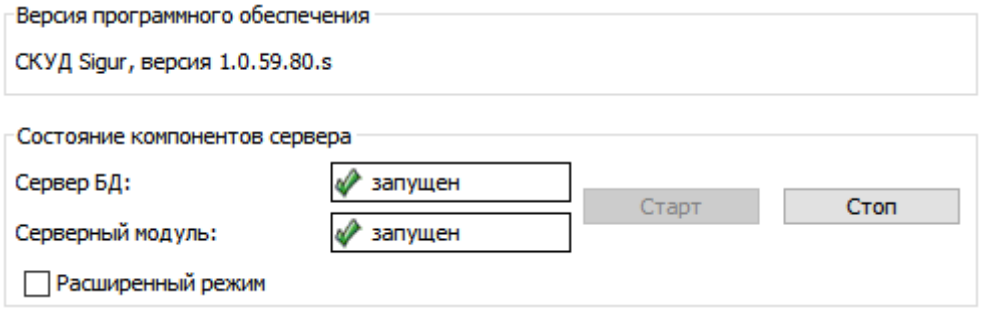


Рис. 14. Обычный режим управления компонентами сервера

Расширенный режим управления компонентами сервера:

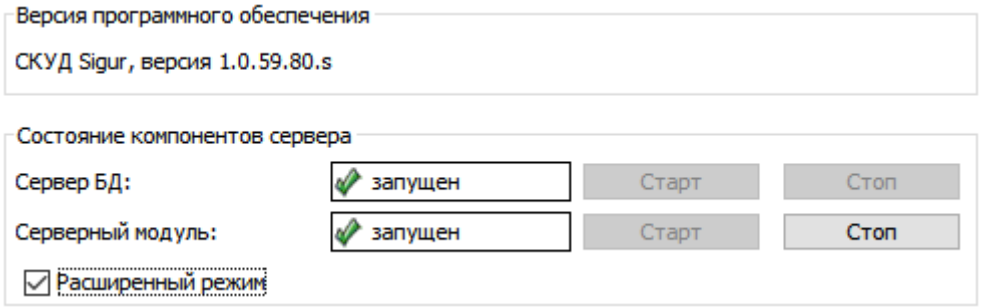


Рис. 15. Расширенный режим управления компонентами сервера

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».

8.1. Управление сервером БД

Запуск сервера БД осуществляется кнопкой «Старт» в строке «Сервер БД».
При первом после установки программного обеспечения запуске сервера БД откроется окно с запросом о создании новой базы данных.

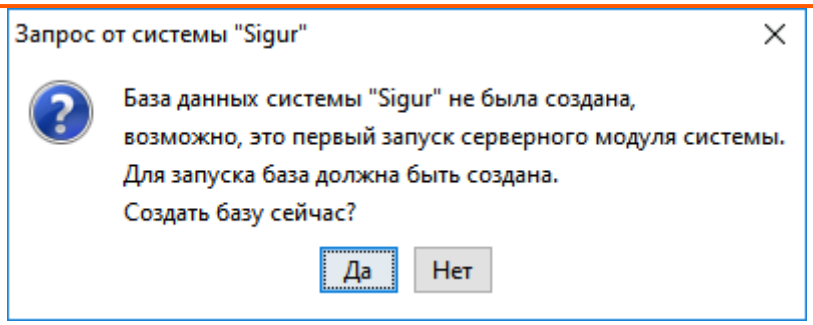


Рис. 16. Окно с запросом создания базы данных

Нажав кнопку «Да», создаём исходную базу данных. База создаётся один раз, и последующие запуски происходят без этого запроса.
Нажав кнопку «Нет», можно отказаться от создания базы данных, при этом сервер БД будет запущен, но работа остальных компонентов ПО при этом невозможна. Для создания БД можно также нажать кнопку «Сбросить базу» во вкладке «База данных».
Остановка сервера БД осуществляется кнопкой «Стоп» в строке «Сервер БД».

8.2. Управление серверным модулем

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

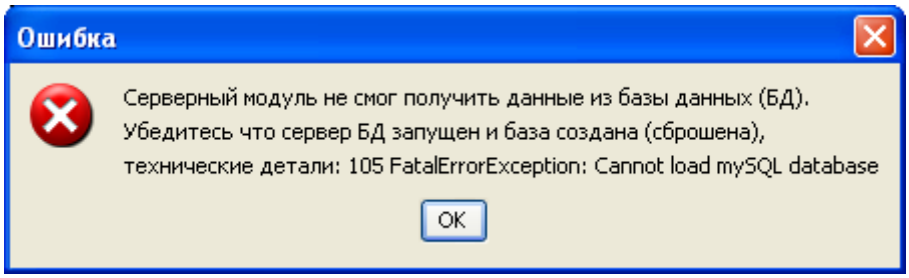


Рис. 17. Сообщение при запуске серверного модуля с повреждённой базой данных

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

9. Управление базой данных

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

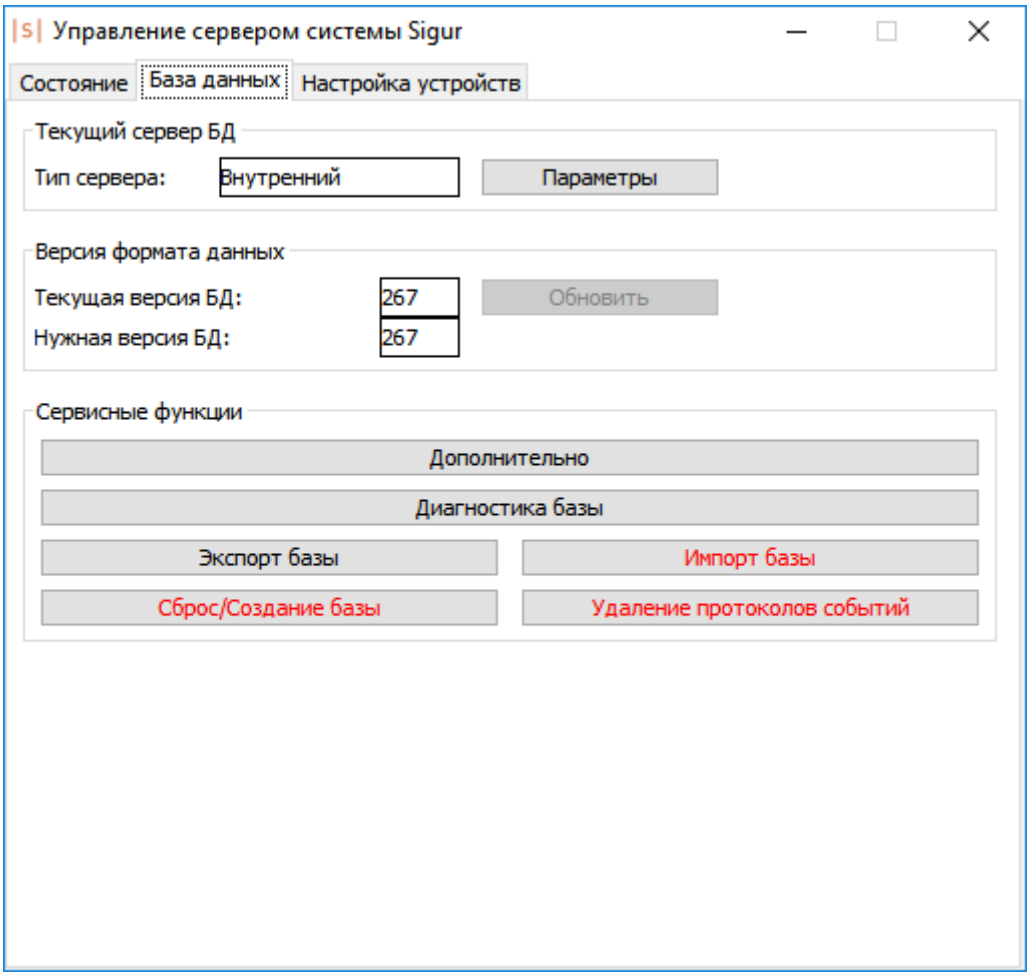


Рис. 18. Окно программы управления сервером, активна вкладка База данных

База данных (БД) используется системой для хранения информации об объектах доступа, режимах допуска, о событиях системы и т.д.
По умолчанию используется встроенная БД MariaDB.

9.1. Версия формата данных

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

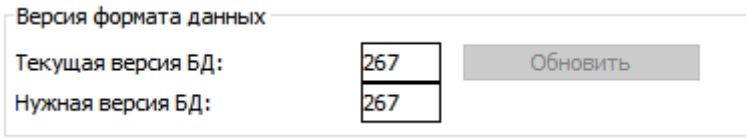


Рис. 19. Панель Версия формата данных

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.

9.2. Обновление версии БД

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».

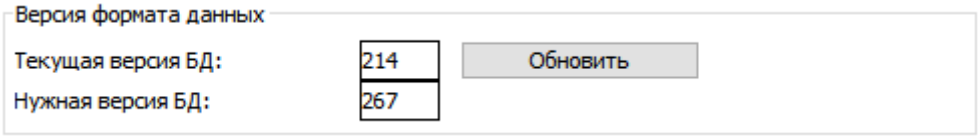


Рис. 20. Пример отличия версий БД

Для обновления текущей версии БД нужно нажать кнопку «Обновить».
Программа откроет окно «Обновляем версию базы», в котором будет отображаться процесс обновления. После успешного завершения процесса окно закроется.
Если обновление программного обеспечения или импорт старой версии базы данных были сделаны при остановленном сервере БД, то при первом же запуске сервера программа выдаст запрос на обновление версии базы данных.

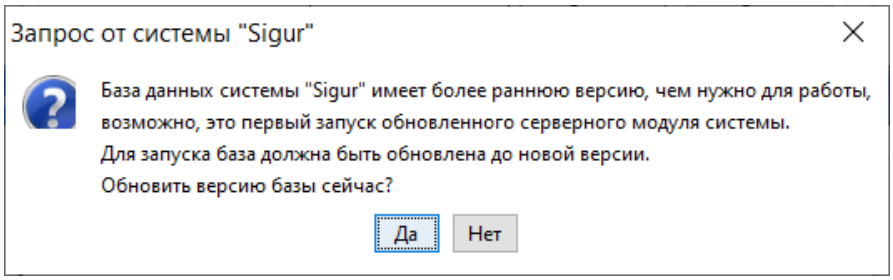


Рис. 21. Сообщение при запуске сервера БД после обновления серверного ПО

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

9.3. Установка пароля на доступ к БД для сторонних программ.

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

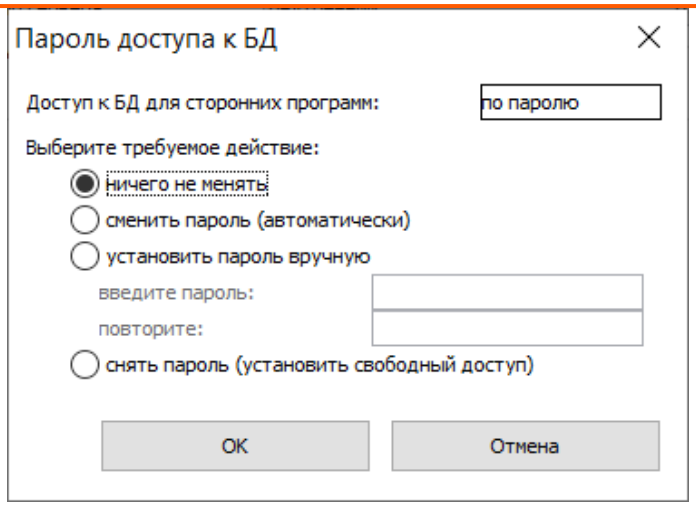


Рис. 22. Окно Пароль доступа к БД

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

- «ничего не менять».

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

- «сменить пароль (автоматически)».

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

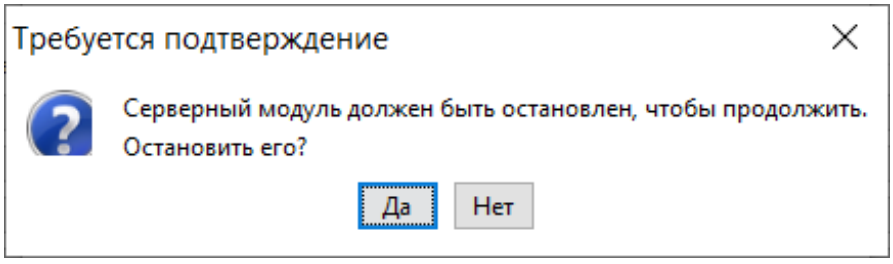


Рис. 23. Окно подтверждения остановки серверного модуля

- «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».

9.4. Дополнительные настройки сервера

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

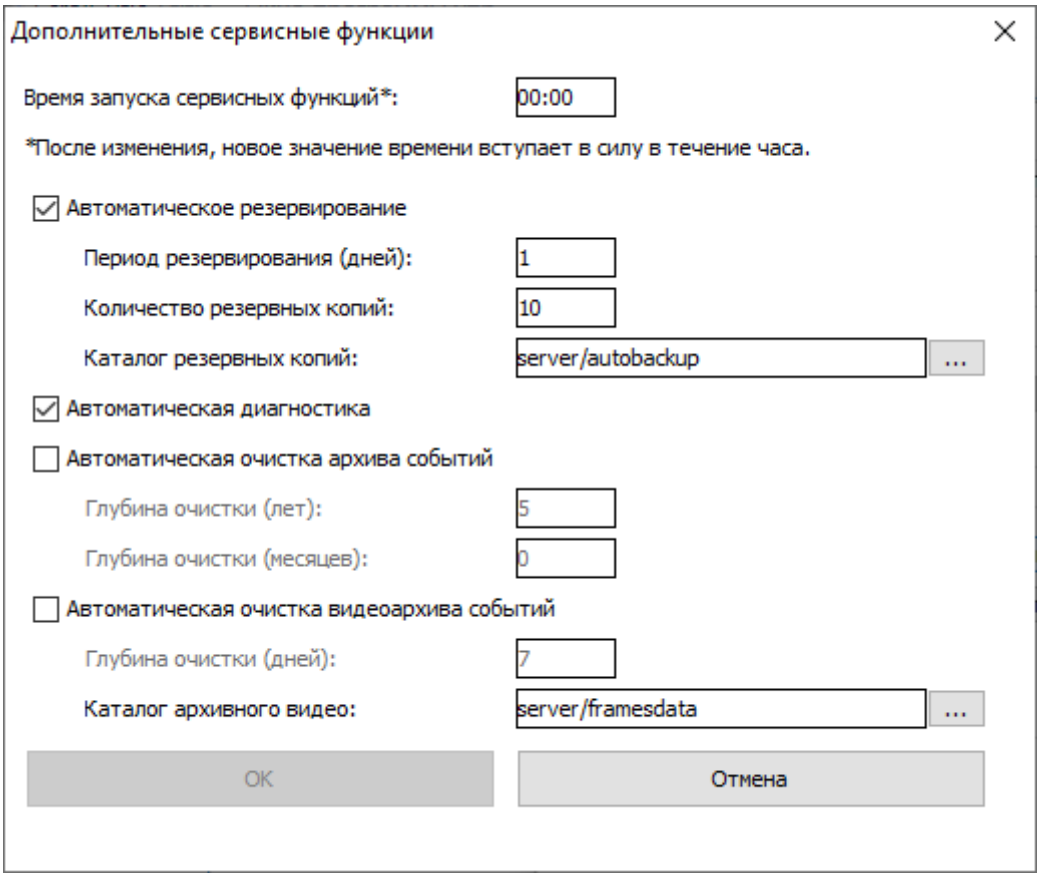


Рис. 24. Дополнительные функции сервера

9.5. Автоматическое резервирование (сохранение) БД

Автоматическое резервирование БД необходимо для создания копий, которые в дальнейшем можно использовать для восстановления БД после серьёзного сбоя, вызвавшего повреждение файловой структуры, или для переноса сервера системы на другой компьютер. Для включения автоматического сохранения БД необходимо:

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

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

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

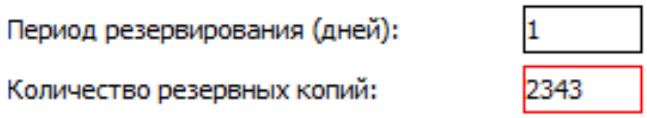


Рис. 25. Пример ввода некорректного значения

По умолчанию резервные копии БД сохраняются программой в каталог установленной программы: «...\SIGUR access management\server\autobackup\», где «...» – путь установки программы (обычно «C:\Program files (x86)\»).
Формат сохраняемых файлов: ГГГГ–ММ–ДД.sql. Название файла определяет год, месяц и день автосохранения.
Старые копии автоматически удаляются..

9.6. Автоматическая диагностика БД

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

9.7. Автоматическая очистка архива событий

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

9.8. Автоматическая очистка видеоархива событий

Для работы данной функции на вкладке «База данных» нажмите кнопку «Дополнительно» и включите опцию «Автоматическая очистка видеоархива событий» и введите нужную глубину очистки видеоархива в днях. Все события видеоархива старше указанного срока будут удаляться.
По умолчанию видеоархив сохраняется программой в каталог установленной программы: «... \SIGUR access management\server\framesdata\», где «...» – путь установки программы (обычно «C: \Program files (x86)\»).

9.9. Сохранение (экспорт) БД

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

9.10. Восстановление (импорт) базы данных

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

Импорт базы данных может потребоваться при переносе системы на другой компьютер или серьёзном сбое, вызвавшем повреждение структуры БД, которое неустранимо с помощью операции «Диагностика базы данных».
Для импорта БД из резервной копии необходимо на вкладке «База данных» нажать кнопку «Импорт базы». Программа запросит подтверждение операции.

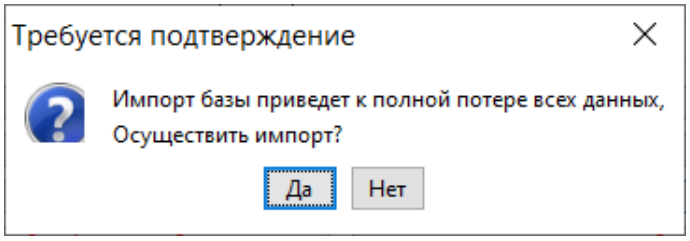


Рис. 26. Запрос подтверждения импорта БД

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.

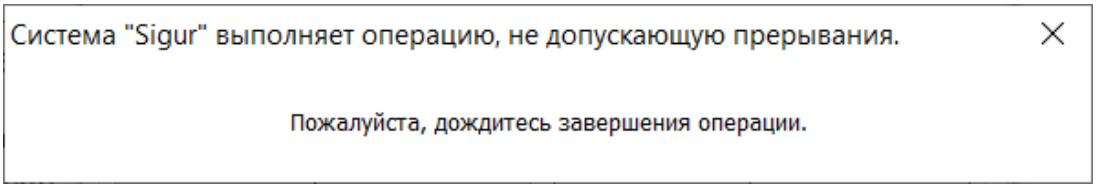


Рис. 27. Информационное окно при импорте базы данных

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».

9.11. Сброс/создание базы данных

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

Выполнение данной операции требуется только в случае необходимости создания чистой базы данных.
Для сброса БД нужно нажать кнопку «Сброс/создание базы». Программа запросит подтверждение потенциально опасной операции.

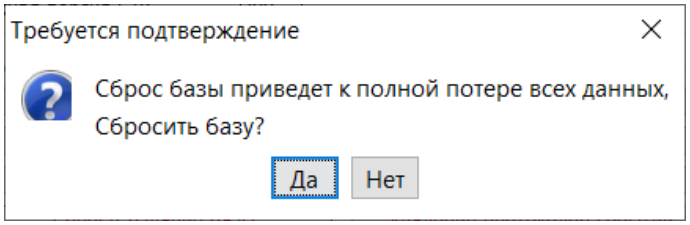


Рис. 28. Запрос подтверждения сброса базы данных

9.12. Диагностика (ремонт) базы данных

Эта функция позволяет устранять некоторые повреждения данных, возникшие, например, в результате аварийного завершения работы системы (зависание, выключение питания компьютера и т.д.).
Следствием таких повреждений является невозможность работы системы. Серверный модуль при этом может выдавать ошибку получения данных.

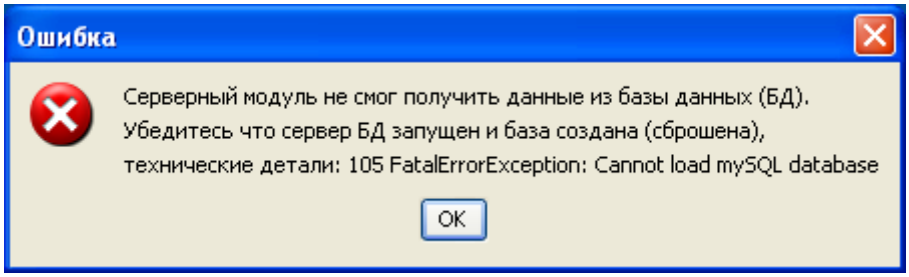


Рис. 29. Ошибка серверного модуля

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

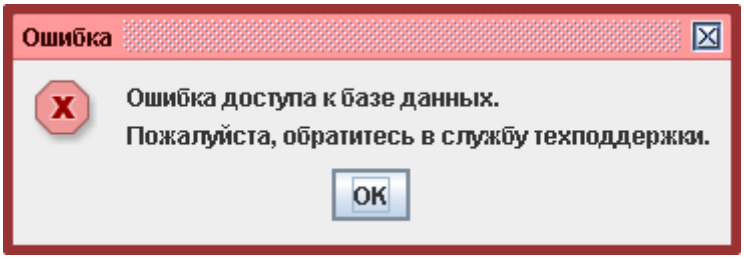


Рис. 30. Ошибка доступа к базе данных

Для исправления повреждений необходимо запустить диагностику, нажав на вкладке «База данных» кнопку «Диагностика базы».
После нажатия откроется окно «Диагностируем базу данных», в котором отображается прогресс операции и комментарии к нему. При успешном окончании процесса это окно автоматически закроется, в случае обнаружения/исправления каких-то серьёзных ошибок окно останется открытым и заполненным сообщениями об обнаруженных проблемах.
Если после этого сообщения об ошибках продолжают появляться – обратитесь в службу технической поддержки.

9.13. Удаление протоколов событий

Эта функция позволяет удалять протоколы до определённой даты.
Для удаления на вкладке «База данных» нажмите кнопку «Удалить протоколы событий».
В появившемся окне удаления протоколов доступны следующие данные:

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

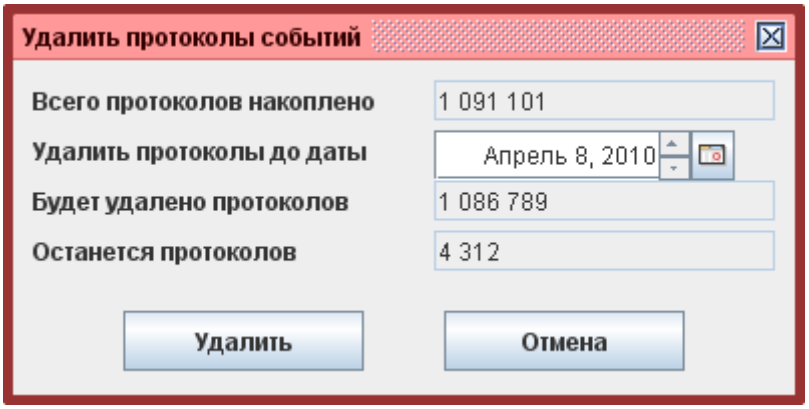


Рис. 31. Окно удаления протоколов событий

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

10. Настройка IP-устройств

На вкладке «Настройка устройств» можно добавлять и перенастраивать контроллеры «Sigur» E серий и IP-турникеты, а также просматривать список доступных на текущий момент в сети устройств.

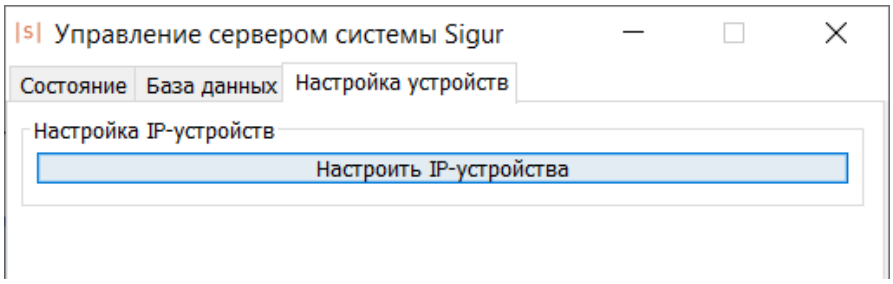


Рис. 32. Вкладка "Настройка устройств".

10.1. 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 нашу техподдержку.

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

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

Запуск программы управления сервером возможен как на сервере СКУД, так и на любом другом компьютере (например, если новый контроллер расположен в другой подсети, до которой не дойдут широковещательные запросы). При этом не требуется запуск компонентов сервера (сервер БД и серверный модуль), вкладка «Настройка устройств» работает автономно, не требует наличия лицензий.

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

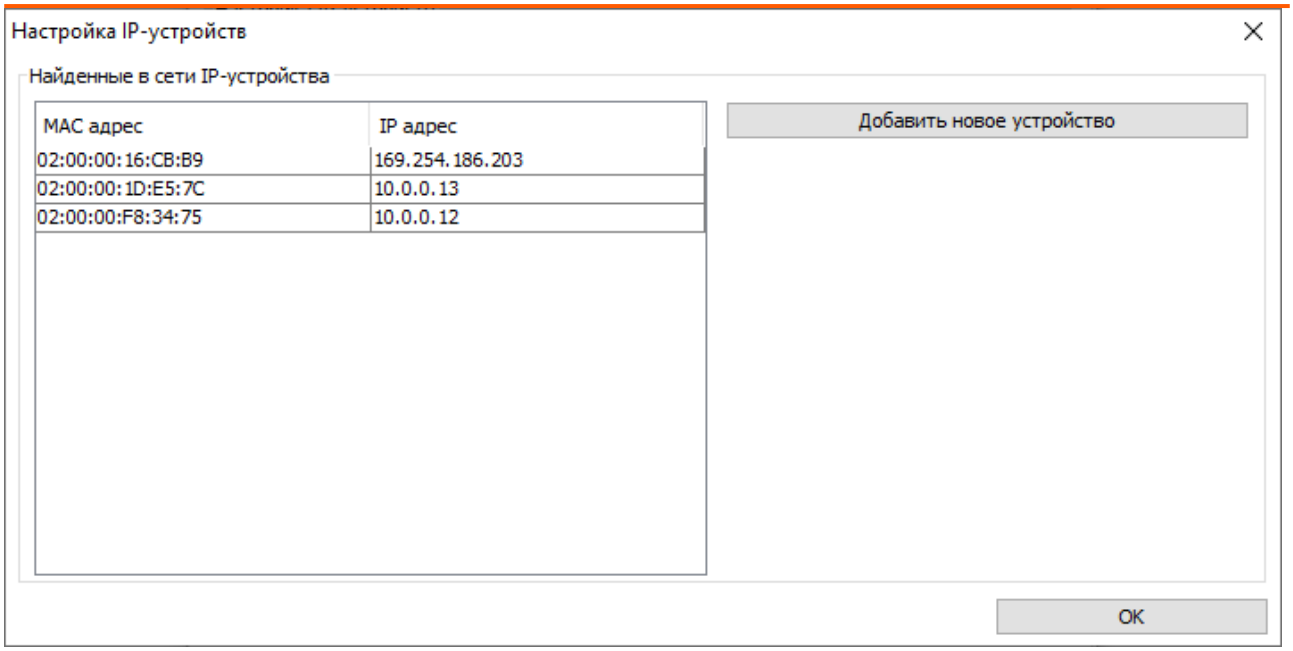


Рис. 33. Список найденных в сети IP устройств.

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

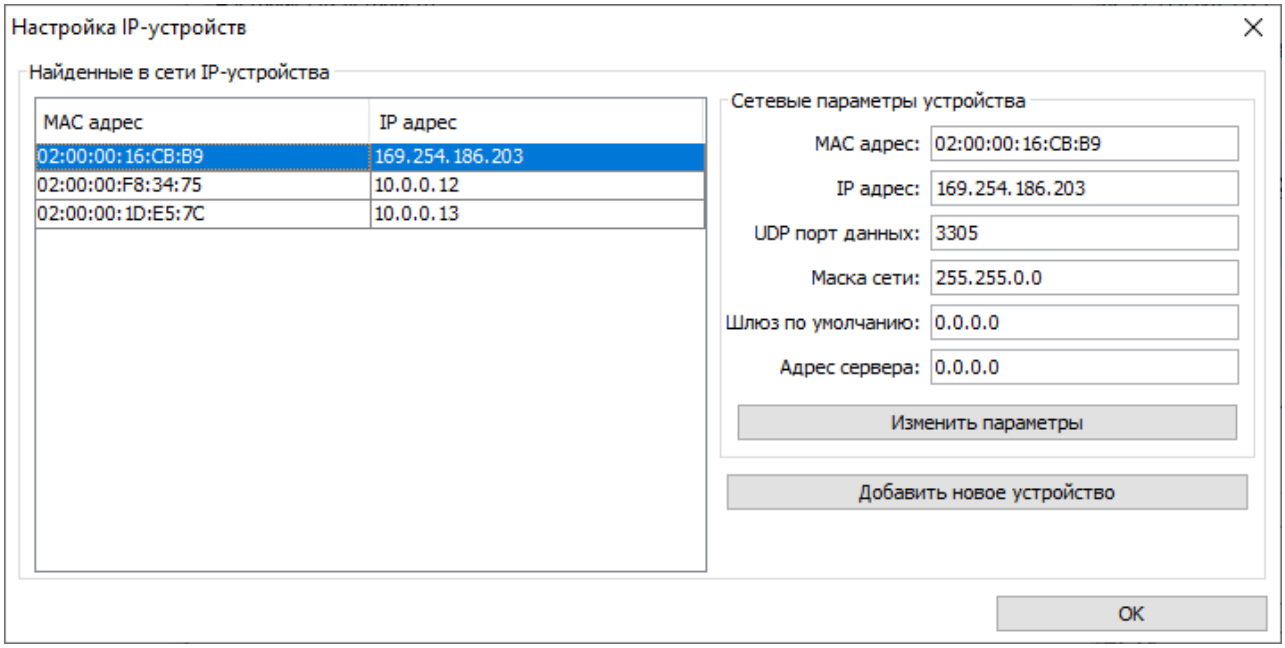


Рис. 34. Параметры выбранного устройства в списке найденных в сети IP-устройств.

Далее возможны два варианта.

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

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

10.1.1. Добавление нового устройства

Введите в соответствии с настройками вашей сети следующие параметры:

- MAC адрес

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

- IP адрес.

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

- 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 «К серверу, 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 «К другому IP-устройству », и введите адрес настоящего сервера.

- Пароль.

Значение пароля по умолчанию уже введено в поле.

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

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

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

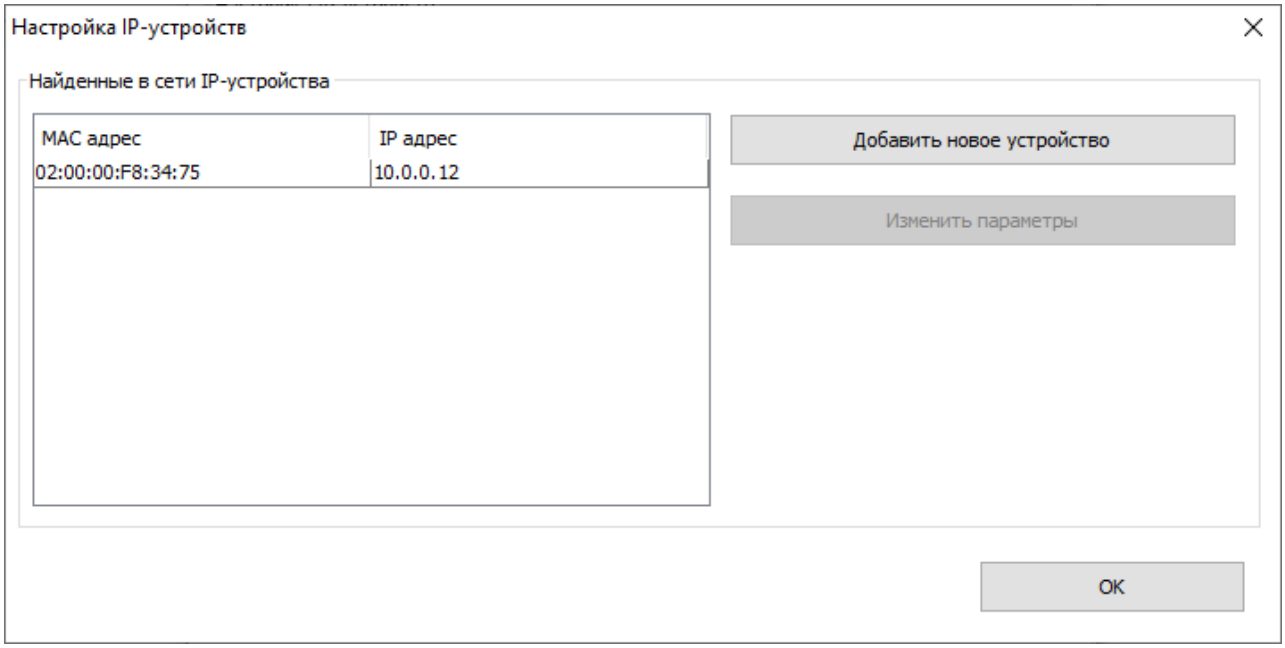


Рис. 35. Успешно настроенный контроллер.

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

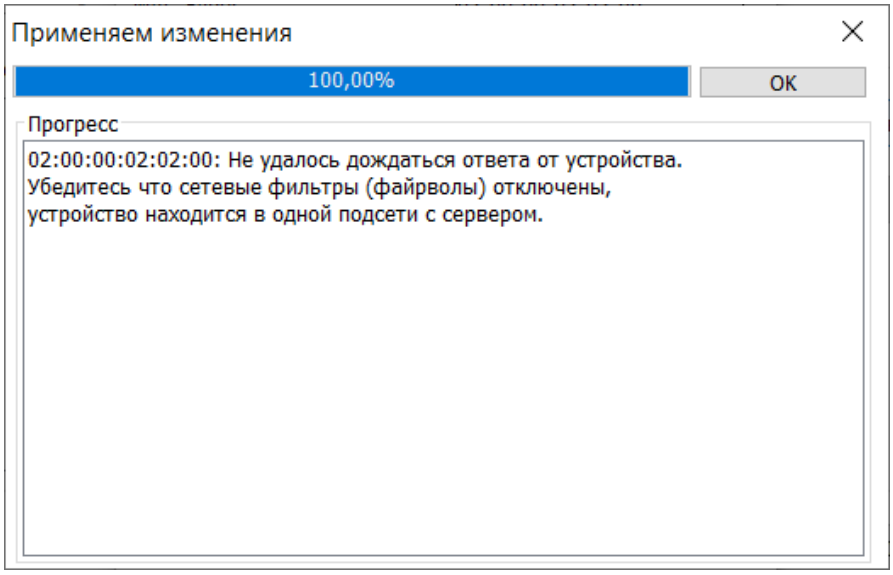


Рис. 36. Ошибка при попытке настройки IP параметров.

10.1.2. Изменение IP-параметров устройства

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

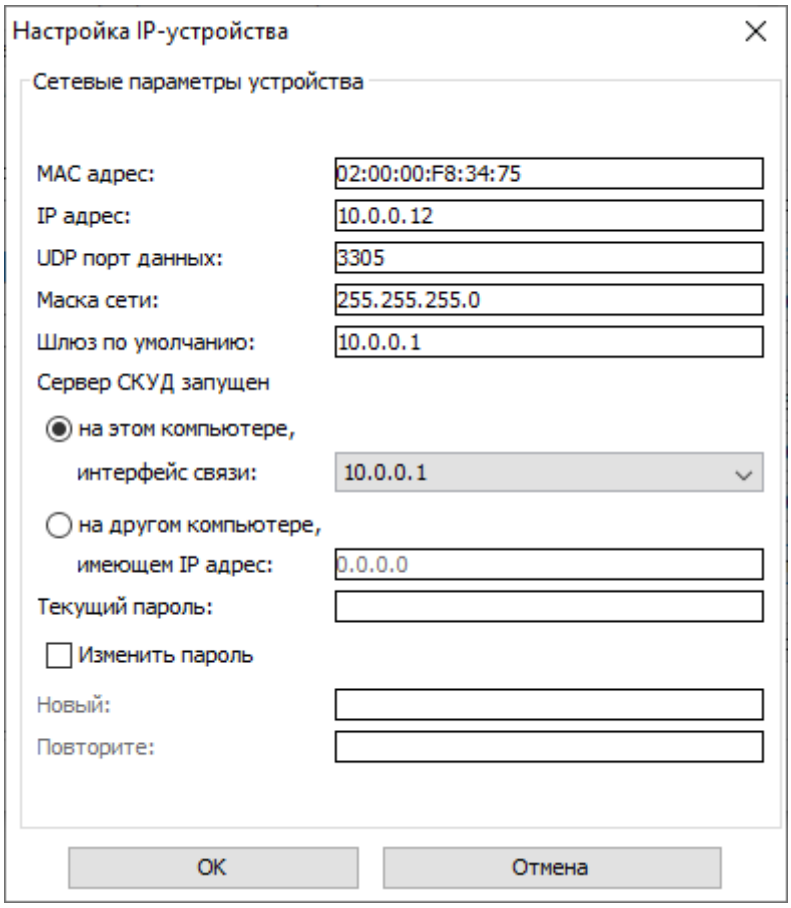


Рис. 37. Окно «Настройка IP-устройства», вариант 1.

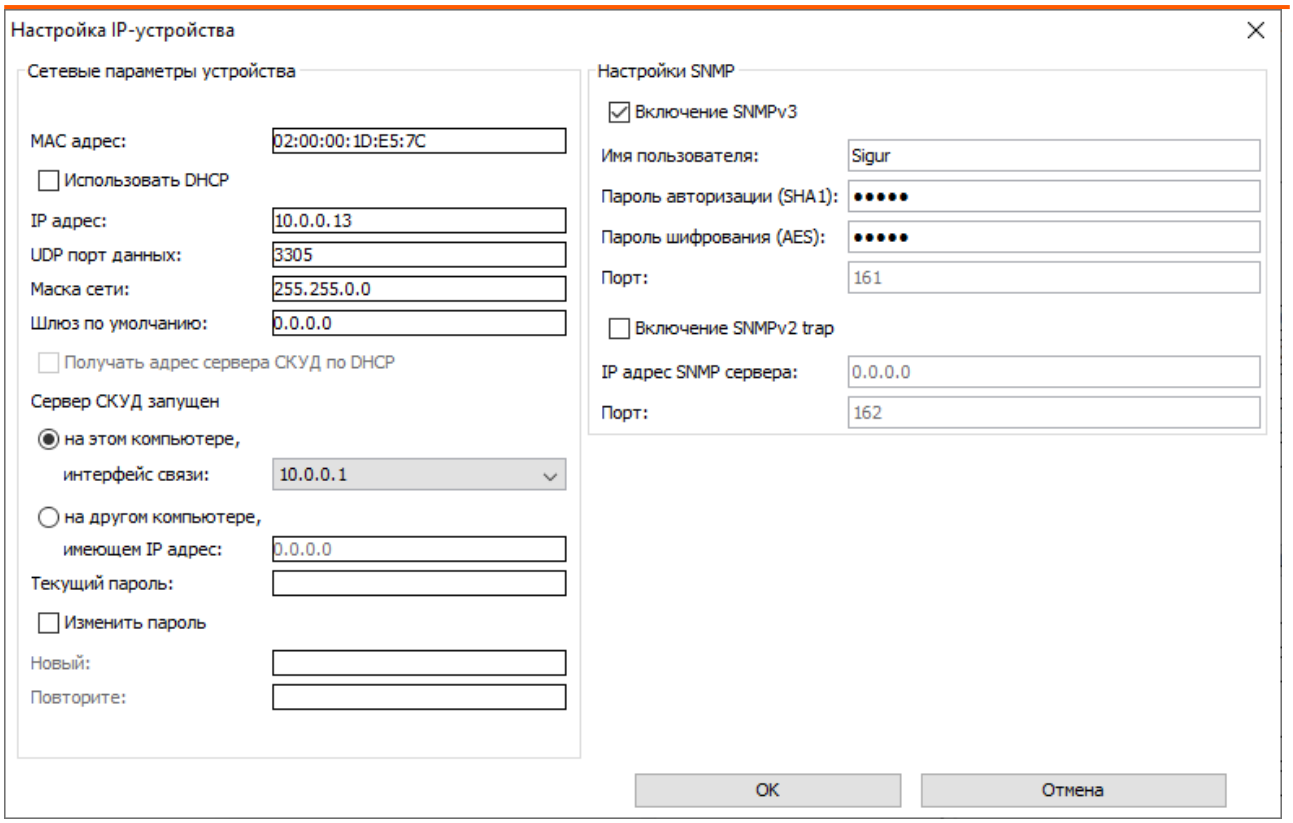


Рис. 38. Окно «Настройка IP-устройства» вариант 2.

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

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

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

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

Получение IP-параметров по DHCP

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

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

Передача статусов SNMP-серверу

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

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

10.2. Возможные причины неудачной настройки IP параметров

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

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

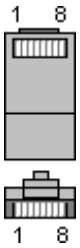


Рис. 39. Нумерация контактов разъёма RJ-45.

Рис. 40. «Прямой» кабель для соединения с помощью коммутаторов.

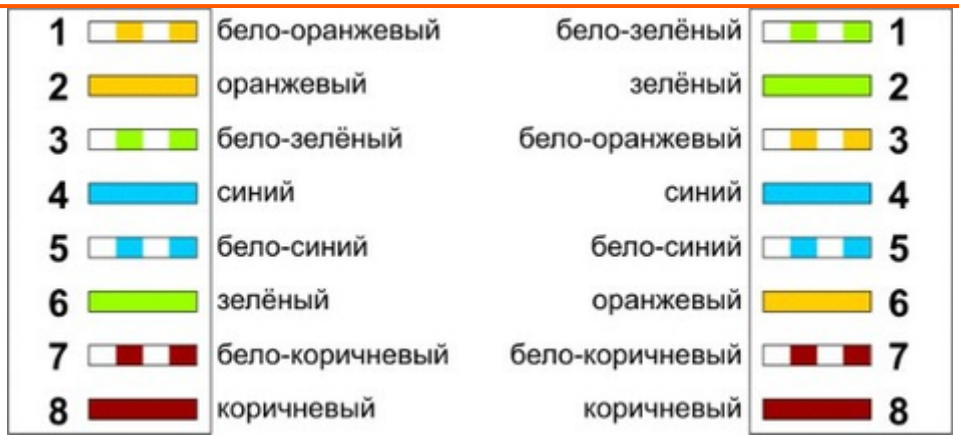


Рис. 41. «Перекрёстный» кабель для соединения «компьютер — контроллер».

- Некорректные настройки сетевых интерфейсов Windows.

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

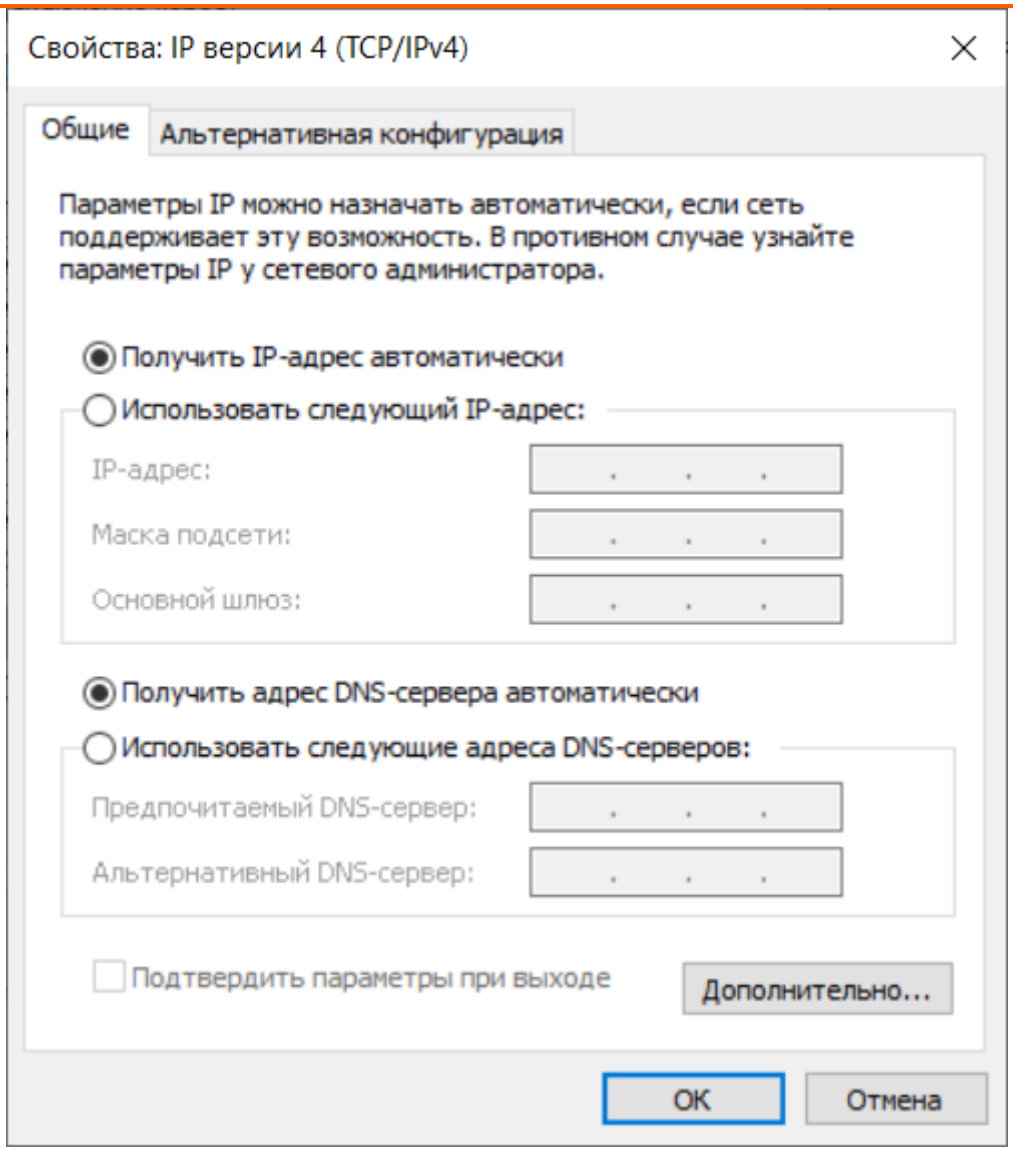


Рис. 42. Неправильные настройки сетевого интерфейса для подключения контроллера.

Пример корректной настройки сервера и контроллера приведён ниже.

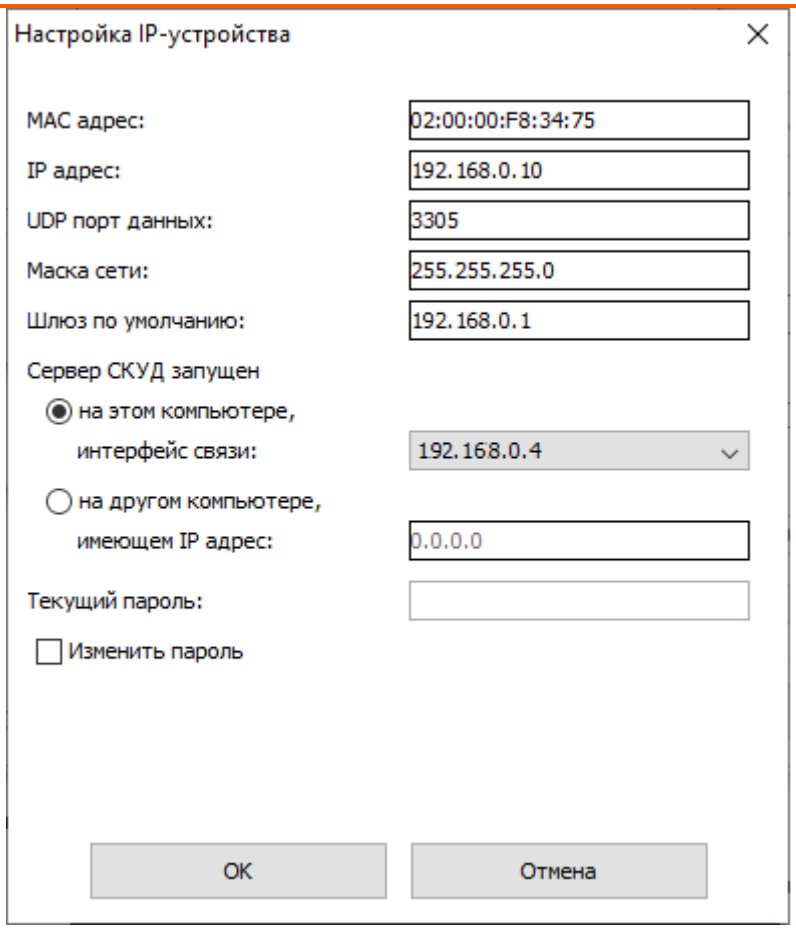


Рис. 43. Пример правильной настройки контроллера

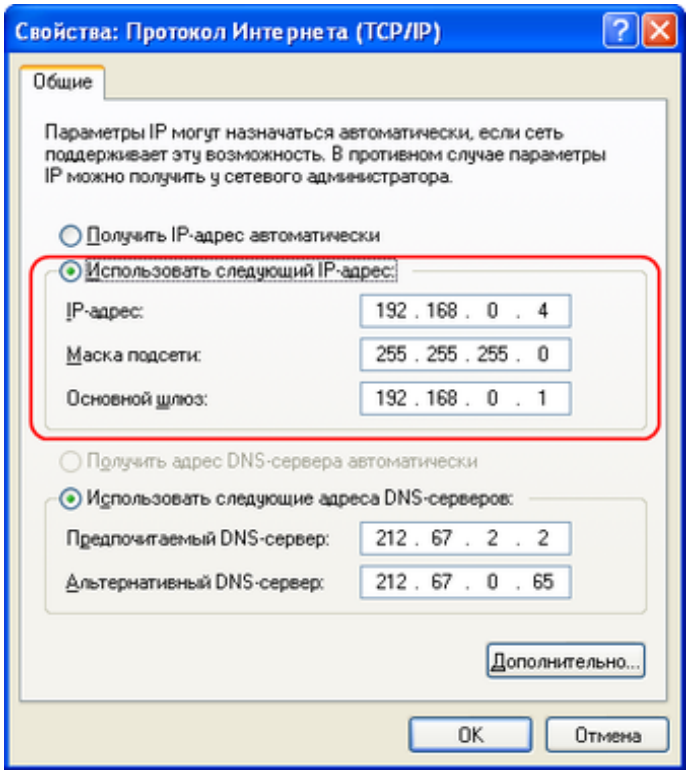


Рис. 44. Пример правильных настроек сетевого интерфейса сервера

- Активность сетевых фильтров либо антивирусов.

Например, встроенный брандмауэр Windows иногда блокирует работу программы с сетевым интерфейсом без уведомления об этом пользователя. На время настройки желательно отключить все программы, которые могут блокировать работу другого ПО или доступ к различным портам.

- Конфликт IP-адресов в сети.

При отсутствии связи с контроллером на вкладке «Оборудование» клиентского места Sigur (контроллер при этом виден в списке «Найденные в сети IP-устройства» программы управления сервером и может успешно пинговаться) 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.

11. Возможные сообщения об ошибках при запуске серверного модуля

- Серверному модулю не удалось прочитать свой конфигурационный файл, технические детали: ...
- Серверный модуль отрапортовал некорректное значение конфигурационного параметра Com, технические детали: ...

Эти ошибки не должны появляться, если не изменять вручную файлы программы.

- 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.
- 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: ...

Эти ошибки выдаются при попытках запуска серверного стандартного (т. е. платного) ПО без ключа HASP.

12. 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.

12.1. Пример работы со встроенным брандмауэром Windows

В случае работы встроенного файрвола ОС Windows XP (SP2 и выше) при запуске ПО «Sigur» с правами администратора системы происходит автоматическое разрешение работы компонентов ПО. В некоторых случаях возможно появление оповещений системы безопасности Windows с запросом, продолжить ли блокирование программы. Для нормальной работы ПО нужно нажать кнопку «Разблокировать».

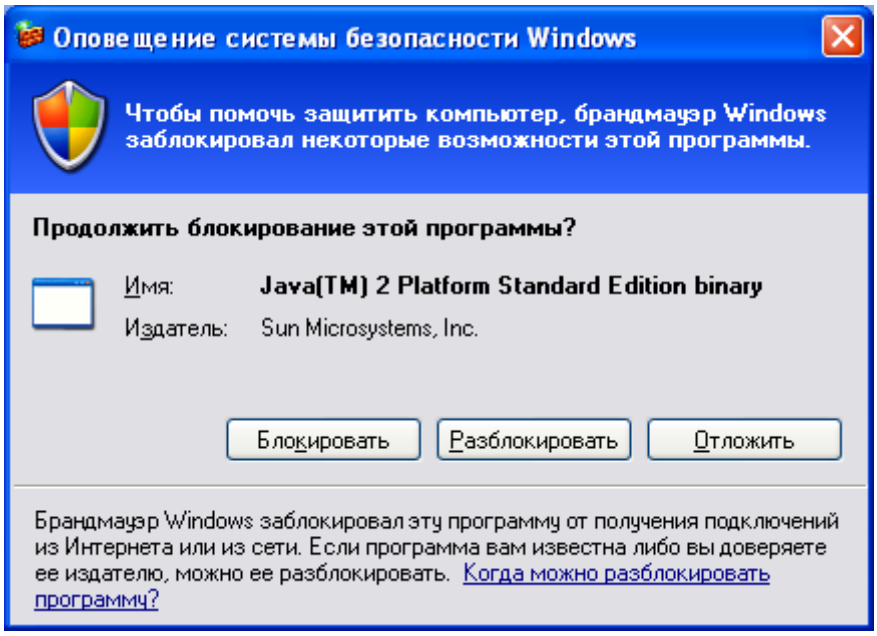


Рис. 45. Пример сообщения брандмауэра Windows.

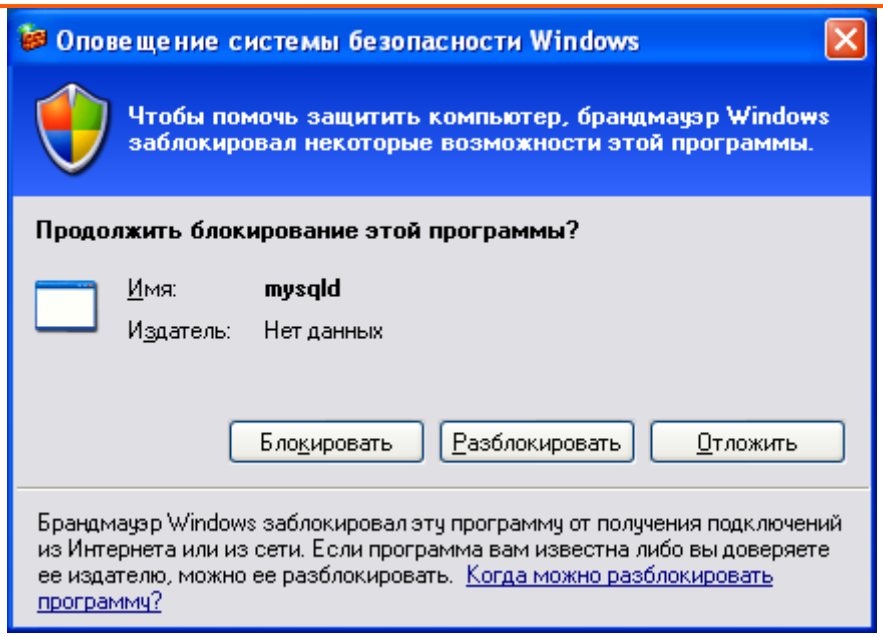


Рис. 46. Пример сообщения брандмауэра Windows, продолжение.

При запуске серверной части ПО «Sigur» с правами ниже, чем права администратора, работа программы будет заблокирована, при этом появится следующее сообщение.

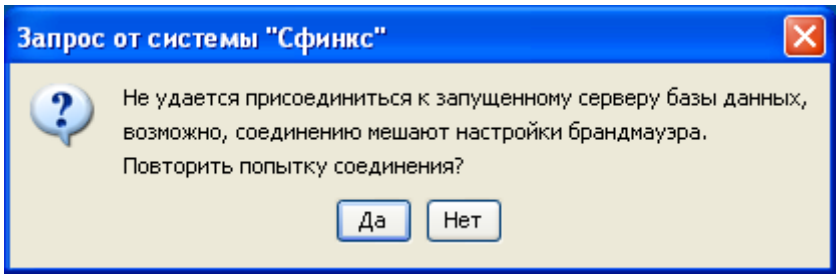


Рис. 47. Сообщение ПО "Sigur" при блокировании его работы файрволом.

При работе с правами ниже, чем права администратора, ограничено изменение многих системных файлов, поэтому возможно появление следующего сообщения об ошибке.

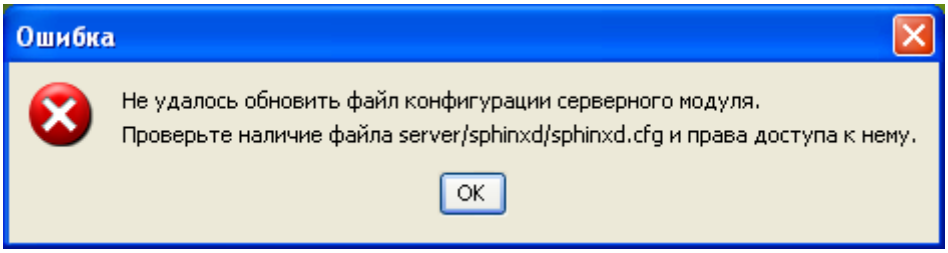


Рис. 48. Сообщение об ошибке при работе с правами ниже, чем права администратора.

Для нормальной работы необходимо войти в систему с правами администратора.
Запуск клиентской части ПО не требует дополнительных настроек файрвола.

12.2. Работа с брандмауэром «ZoneAlarm Pro»

При работе на компьютере файрвола «ZoneAlarm Pro», настроенного на автоматическое обучение, в процессе установки и при первых запусках СКУД «Sigur» будут появляться запросы от файрвола на блокирование программы.

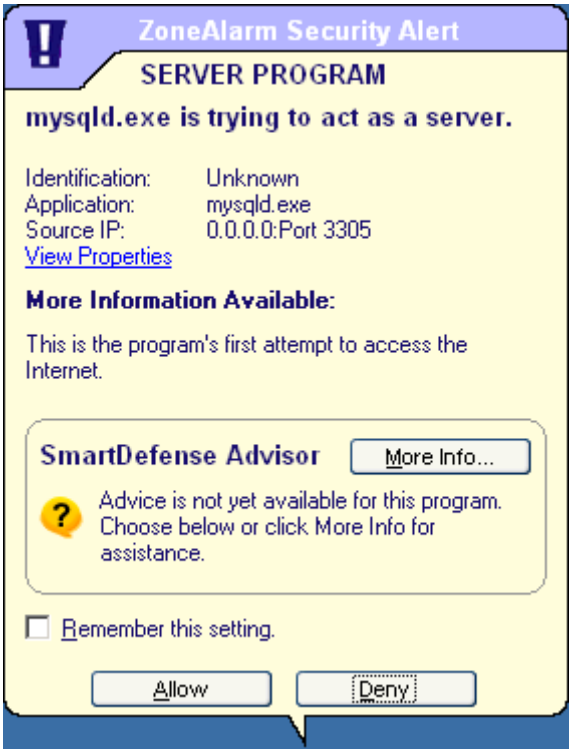
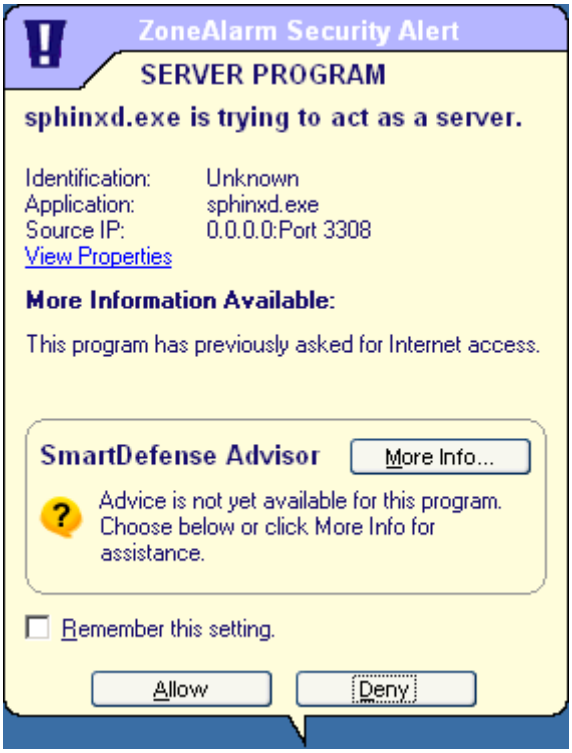
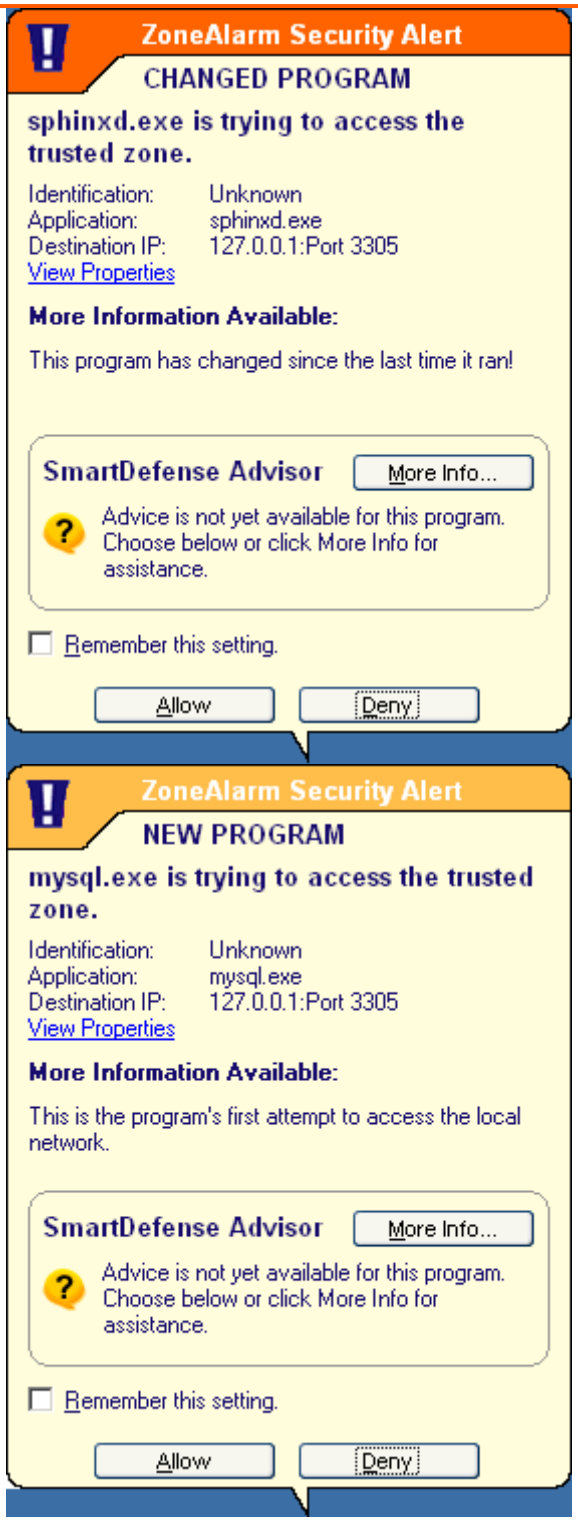


Рис. 49. Примеры запроса файрвола на блокирование/разблокирование программы.




ZoneAlarm Security Alert
CHANGED PROGRAM
sphinxd.exe is trying to access the trusted zone.
Identification: Unknown
Application: sphinxd.exe
Destination IP: 127.0.0.1:Port 3305
View Properties
More Information Available:
This program has changed since the last time it ran!
SmartDefense Advisor
More Info...
Advice is not yet available for this program. Choose below or click More Info for assistance.
Remember this setting.
Allow
Deny
ZoneAlarm Security Alert
NEW PROGRAM
mysql.exe is trying to access the trusted zone.
Identification: Unknown
Application: mysql.exe
Destination IP: 127.0.0.1:Port 3305
View Properties
More Information Available:
This is the program's first attempt to access the local network.
SmartDefense Advisor
More Info...
Advice is not yet available for this program. Choose below or click More Info for assistance.
Remember this setting.
Allow
Deny

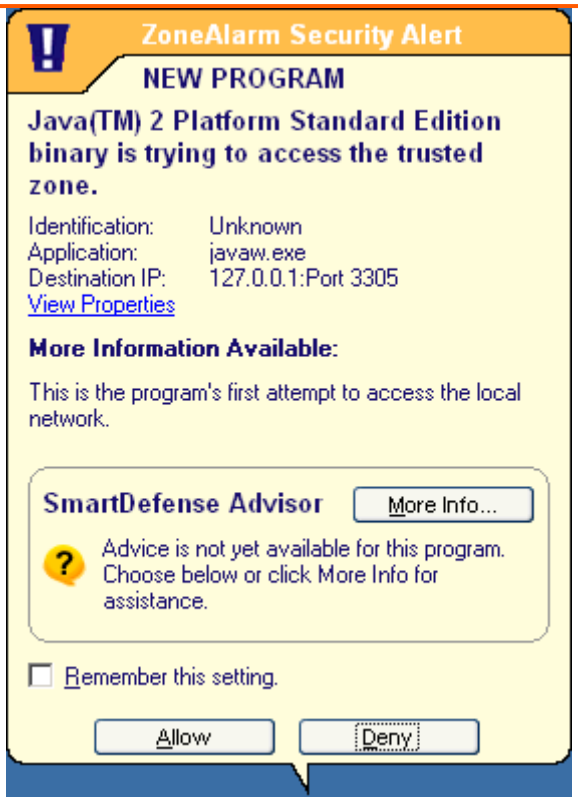


Рис. 50. Пример запроса файрвола на блокирование/разблокирование программы, продолжение.

Для продолжения нормальной работы ПО «Sigur» необходимо в каждом появляющемся окне выделять пункт «Remember this setting» и после этого нажимать на кнопку «Allow».

Рис. 51. Необходимые действия в появляющихся окнах запроса.

В итоге автоматического обучения в закладке «Program control» файрвола должны появиться следующие строки:

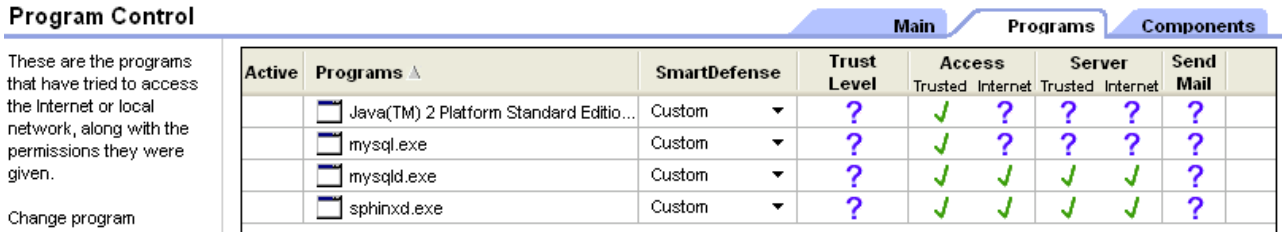


Рис. 52. Модули СКУД «Sigur» в списке «Programs» файрвола.

В дальнейшем запросы от файрвола могут появляться только в случае обновления программы.

13. 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.

Таблица 1. TCP порты, используемые системой по умолчанию.

Номер порта	Для чего используется
3305	Для связи с клиентскими местами и подключения к базе данных.
3308	Для связи с клиентскими местами и NFC-терминалом.
3312	Для предоставления доступа к серверу по протоколу открытого интерфейса.
3314	Для передачи кадров IP-камер на клиентские места.

Таблица 2. UDP порты, используемые системой по умолчанию.

Номер порта	Для чего используется
3303	Для обмена управляющими сообщениями.
3305	Для информационного обмена с контроллерами.

ООО «Промышленная автоматика – контроль доступа»

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