ООО «Компания Семь Печатей»

117216, Москва, ул. Феодосийская, д. 1, корп. 6; тел.(факс): (495)225-25-31, (495)020-23-46

Email: 2252531@mail.ru; Web-page: www.sevenseals.ru, www.shop-sevenseals.ru

Система
контроля и управления доступом

TSS-OFFICE

TSS-PROFI

***ВЕРСИЯ** 7*

Программное обеспечение

Подсистема управления электронными замками фирмы ASSAAbloyAperio (TSSAbloy)

руководство администратора

Москва

2017

Оглавление

Подсистема работы с электронными замками позволяет включать в состав СКУД TSS2000 Profi беспроводные электронные замки (цилиндры) фирмы Abloy.

Для использования в рамках СКУД электронных замков необходим контроллер управления TSS2010-DV, который обеспечивает автономную работу подсистемы (не зависящую от наличия связи с главным Сервером СКУД).

1. Архитектура системы

На рисунке представлена примерная схема построения сети СКУД с использованием электронных замков фирмы Abloy.

Сами замки встраиваются в двери, как обычные цилиндры (личинки) для механических замков. С внешней стороны такой цилиндр снабжен считывателем бесконтактных карт, с внутренней – ручкой, позволяющей свободно открыть дверь. Разблокировка замка с внешней стороны производится только по команде со стороны управляющей СКУД[1].

С управляющей СКУД замки связываются через ретрансляционное устройство – хаб. Связь цилиндра с хабом беспроводная, по радиоканалу. Связь хаба с управляющим компьютером (контроллером) – по интерфейсу RS 485 или по IP-каналу. В данной системе используются хабы с подключением по RS 485, как наиболее надежному.

Один хаб может обслуживать до 8 цилиндров (замков).

Для управления электронными замками используется специальный контроллер (TSS2010-DV), обеспечивающий их работоспособность в автономном режиме, т.е. без участия сервера СКУД. Сервер СКУД позволяет конфигурировать систему, загружать ключи и права доступа и принимать события о проходах через двери, оснащенные электронными замками (точно так же, как он выполняет эти действия для обычных исполнительных элементов СКУД).

[1] В памяти личинки может содержаться не более десяти так называемых аварийных ключей – для разблокировки двери при отсутствии связи со СКУД.

Полная информация о проектировании, монтаже и настройке сети электронных замков фирмы Abloy содержится в документации разработчика.

Настройка и конфигурирование системы выполняется на трех уровнях:

- Настройка электронных замков и хабов.
- Настройка управляющего контроллера.
- Настройка Сервера СКУД.

Первоначальная настройка замков выполняется программой *Aperio Programming Application*. Главная ее задача – задать корректные адреса цилиндров, поскольку адрес каждого электронного замка является уникальным в системе (по меньшей мере, в пространстве адресов управляющего контроллера) и находится в диапазоне от 1 до 255.

Эта программа также позволяет занести в память цилиндра аварийные ключи и выполнить ряд дополнительных настроек (тип считываемой карты, время срабатывания реле, частота радиоканала и прочие).

Программа *Aperio…* может быть установлена на любом ПК, для ее работы необходим USB-ключ производителя. Связь с настраиваемыми электронными замками осуществляется по радиоканалу непосредственно между USB-ключом и хабами.

Следующий уровень – создание автономной системы контроля доступа по электронным замкам на управляющем контроллере TSS2010-DV посредством ПО *TSSAbloy*. Программа может работать на любом сетевом ПК, однако предпочтительнее запускать ее на Сервере СКУД.

Программа *TSSAbloy* конфигурирует единую систему контроля доступа для всех дверей, оснащенных электронными замками. После этого система может функционировать под управлением отдельного управляющего контроллера без связи с центральным сервером СКУД. Говоря другими словами – если СКУД включает в себя только пункты прохода с электронными замками, и у пользователя системы нет необходимости получать информацию о работе СКУД в режиме реального времени, то система уже может работать в автономном режиме.

Если двери с электронными замками являются частью более глобальной системы контроля доступа, а также если необходим постоянный мониторинг ее работы с оперативным изменением базы владельцев ключей и их прав доступа, то следует выполнить **верхний уровень** настроек – с помощью программы СКУД *Конфигуратор*. Однако, даже при работе в комплексном режиме, система (или, точнее, подсистема) электронных замков все равно будет управляться «своими» контроллерами, вне зависимости от работоспособности ПО верхнего уровня и связи с сервером СКУД.

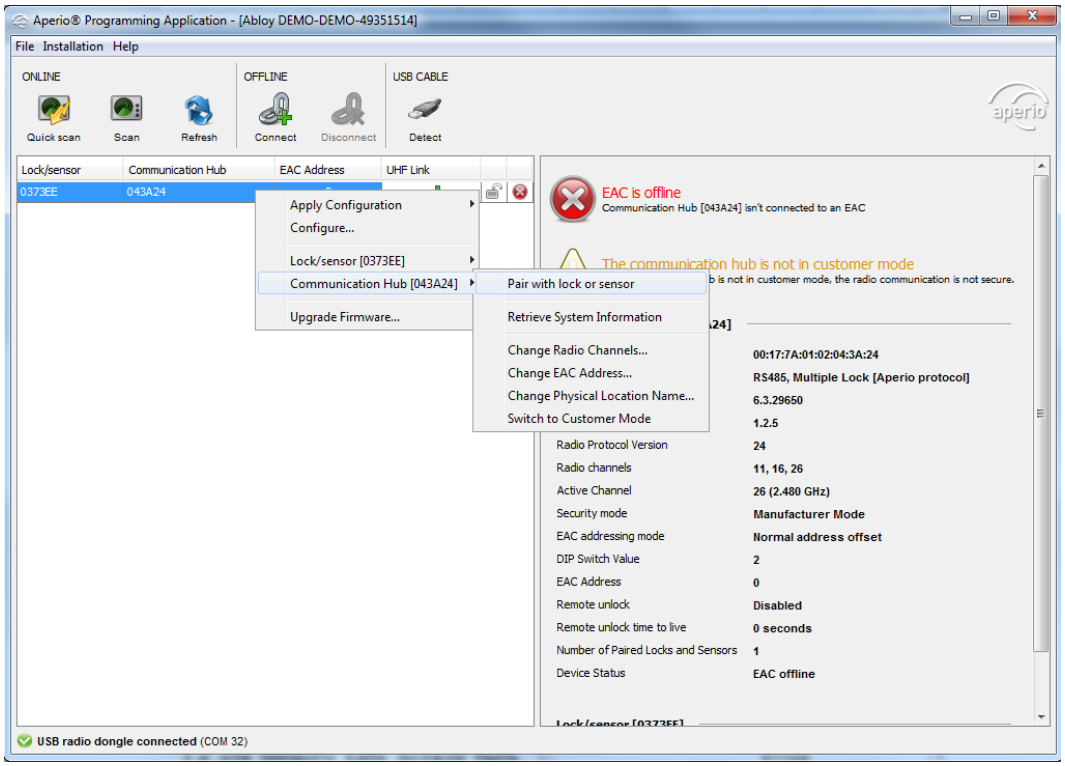
2. Настройка и конфигурирование системы (общие принципы)

2.1. Настройка электронных замков и хабов

Первоначальная настройка системы осуществляется сразу после ее монтажа[2] (или параллельно монтажу) с помощью ПО *Aperio Programming Application* и документации к ней (*ST-001322 Aperio Online Quick Installation Guide-D.pdf* и*ST-001322 Aperio Online Quick Installation Guide-D.pdf*).

Для конфигурирования и запуска системы в целом достаточно на первом этапе оставить все параметры электронных замков по умолчанию, обратив при этом внимание на задание адресов цилиндров.

Для указания хабу с какими цилиндрами он должен работать следует пользоваться пунктом контекстного меню Pair with lock or sensor. При этом хаб соединится со всеми замками, которые окажутся в зоне видимости.



Если в системе используется один хаб, то для каждого из восьми цилиндров адреса будут выглядеть так (арифметическая прогрессия с шагом 16)[3]:

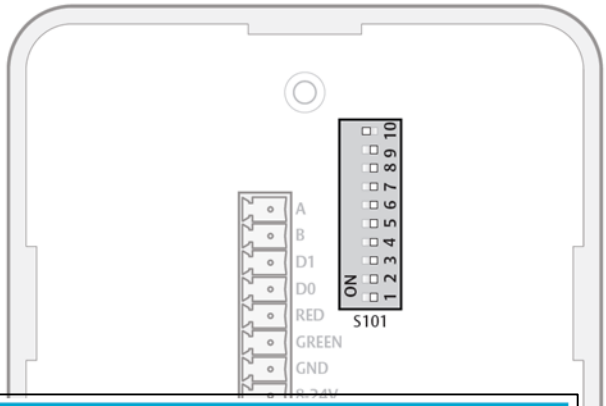
1-ый хаб: 1, 17, 33, 49, 65, 81, 97, 113.

[2]Монтаж выполняется согласно документу ST-001323-Aperio Online Mechanical Installation Manual-C.pdf.

[3] Адреса здесь приведены в десятичной системе, в фирменной документации большей частью используется шестнадцатеричная система.

При наличии на 485 шлейфе более одного хаба необходимо вручную, с помощью DIP переключателей, выставить их адреса, так указано в таблице[4].

Т.е для первого хаба должен быть выставлен в положение ON переключатель 1, для второго – переключатель 2, для третьего включены оба первых переключателя и так далее.



После выставления адресов следует выполнить описанную выше процедуру поиска цилиндров. Результатом этого станут такие последовательности:

DIP 5 – DIP 1	AH30 Hub address	Lock addresses
0000		Reserved
0001	0x01	0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08
0010	0x02	0x09, 0x0A, 0x0B, 0x0C, 0x0D, 0x0E, 0x0F, 0x10
0011	0x03	0x11, 0x12, 0x13, 0x14, 0x14, 0x16, 0x17, 0x18
0100	0x04	0x19, 0x1A, 0x1B, 0x1C, 0x1D, 0x1E, 0x1F, 0x20
...		

2-ой хаб: 2, 18, 34, 50, 66, 82, 98, 114.

3-ий хаб: 3, 19, 35, 51, 67, 83, 99, 115.

Распределенные таким образом адреса будут однозначно указывать на конкретную дверь, поэтому рекомендуется на этом этапе составить план помещений с указанием заданных адресов замков для каждой двери.

Обратите внимание на важность задания корректных адресов в свете дальнейшего конфигурирования: ошибочные адреса повлекут дополнительную работу по реконфигурированию системы.

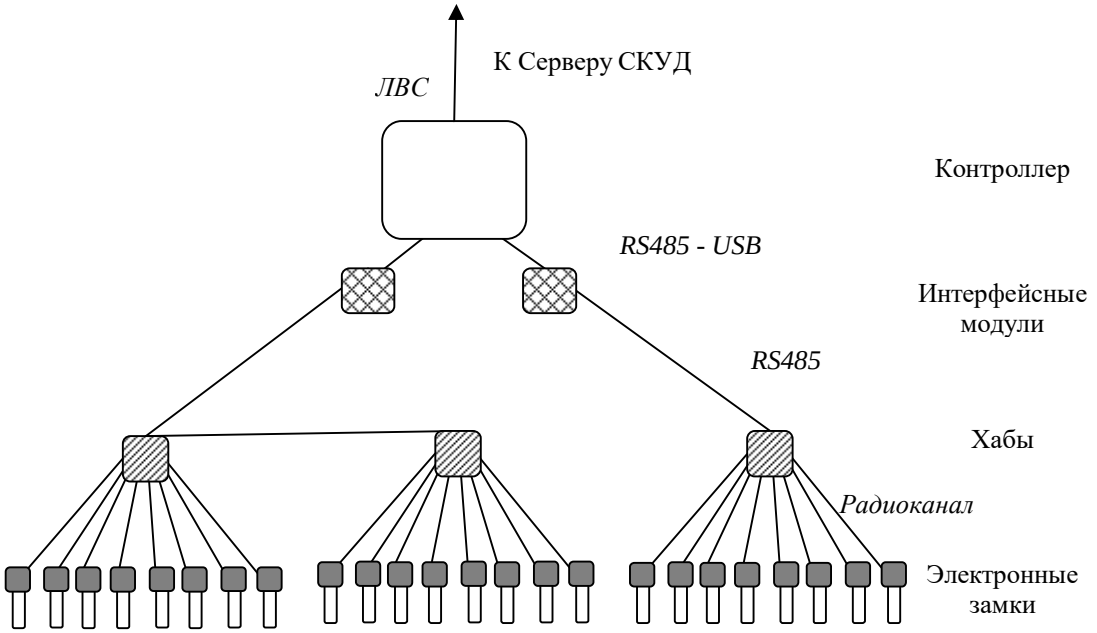
[4] Подробнее читайте в упомянутом документе ST-001323.

2.2. Настройка управляющего контроллера

2.2.1. Физическое подключение устройств

Как уже говорилось, сеть электронных замков состоит из самих дверных замков (цилиндров) и хабов-ретрансляторов, каждый из которых обслуживает до восьми замков.

Хабы подключаются к управляющему контроллеру посредством интерфейсной линии RS 485, которая заканчивается интерфейсным модулем RS 485-USB и заводится на один из 7 USB-портов контроллера.

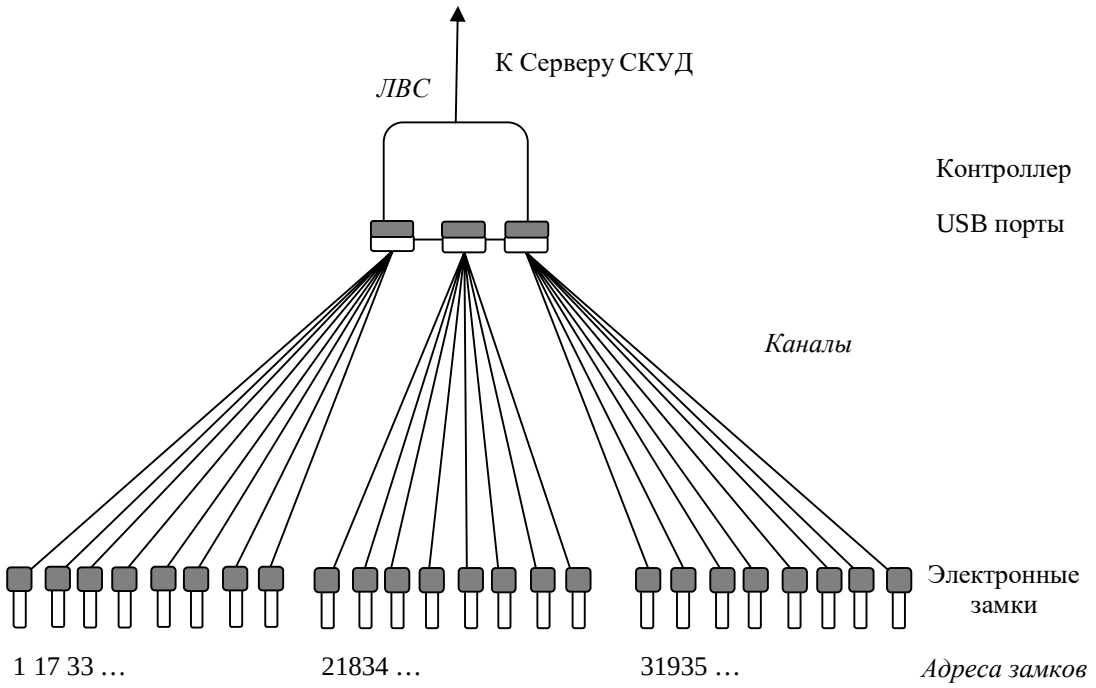


Таких шлейфов может быть несколько, каждый из них заводится на свой USB-порт.

2.2.2. Логическое описание устройств

Управляющий контроллер «не видит» описанного в предыдущем разделе коммутационного оборудования. Он работает непосредственно с электронными замками, разнесенными по нескольким каналам (физическим USB-портам).

На каждом канале может быть не более восьми цилиндров, общее число замков – не более 255. Адресация замков связана с описанным выше правилом назначения адресов при первоначальной настройке системы на уровне хабов. Так, например, для схемы, изображенной на рисунке, адреса всех электронных замков в системе выстроятся в следующей последовательности (вне зависимости от того, каким хабам они принадлежат и на какие порты контроллера заведены): 1, 2, 3, 17, 18, 19, 33, 34, 35.



Вся дальнейшая настройка (равно как и работа) построена исключительно на этих адресах, уникальных для каждого управляющего контроллера.

2.2.3. Создание списка устройств

Список контроллеров и помещений, оснащенных электронными замками, создается в программе *TSSAbloy*, как описано в соответствующих разделах.

Список создается в виде дерева, верхними узлами которого являются контроллеры, а элементами контроллеров – электронные цилиндры (двери или помещения). На этом этапе необходим ранее составленный план, с которого должны быть перенесены адреса замков и их описание.

Данный план понадобится вам и при конфигурировании системы на верхнем уровне, в программном модуле СКУД *Конфигуратор*.

2.2.4. Создание списка пользователей

Программа *TSSAbloy* позволяет создавать и списки владельцев электронных ключей с указанием временн***ы***х и пространственных ограничений их доступа. Эта возможность удобна на этапе отладки системы на уровне автономной работы управ-

ляющего контроллера и необходима, если предполагается только автономная работа, без ПО верхнего уровня. Для присвоения пользователям кода их электронной карты любой из электронных замков может быть активирован в качестве контрольного (регистрирующего) считывателя.

При работе в рамках единой СКУД, информация о владельцах ключей вместе с кодами и правами доступа будет загружаться автоматически при занесении соответствующих данных в программе *Персонал*.

2.3. Настройка Сервера СКУД

Работу подсистемы электронных замков, как части общей СКУД, обеспечивает программный модуль *PSrvc_abloyTSS.exe*, реализованный как служба Windows *TSSAbloy*.

Обмен данными позволяет в режиме реального времени загружать в контроллер информацию о сотрудниках, редактируемых в программе *Персонал* (*Бюро пропусков*). Со стороны контроллера передаются события системы контроля доступа на электронных замках – о проходах или попытках проходов, о состоянии связи с цилиндрами и общей работоспособностью подсистемы.

Принятые ядром СКУД события фиксируются в системном журнале (что позволяет формировать по ним отчеты) и рассылаются клиентам СКУД (программы *Проходная, Дистанционный мониторинг, Управление объектами*) для отображения данных в реальном времени.

В случае разрыва связи между двумя компонентами системы или неработоспособности одного из компонентов данные буферизуются и при восстановлении связи передаются той или другой стороне. Естественно, во время разрыва связи события проходов на дверях с электронными замками не будут отображаться в перечисленных выше программах реального времени.

2.4. Особенности работы подсистемы электронных ключей

Управляющий электронными ключами контроллер **всегда работает в автономном режиме** – и в этом его основное отличие от режима работы стандартных контроллеров СКУД.

Поэтому подсистема с равной функциональностью может работать как автономная, т.е. без средств отображения в реальном времени и возможности быстрой загрузки ключей и изменения прав их доступа, так и как комплексная – т.е. с отображением и управлением в реальном времени.

Для администрирования подсистемы в «автономном»[5] варианте существует программа *TSSAbloy*.

При работе в составе серверной СКУД электронные замки становятся частью общей системы.

Единственно, что не допускается – это одновременная работа в составе СКУД (т.е. с запущенной службой *PSrvc_abloyTSS*) и с помощью программы *TSSAbloy*.

[5] Еще раз подчеркнем, что она работает в автономе (т.е. решения принимает контроллер) всегда; в данном варианте речь идет о невозможности отображать и управлять системой в реальном времени. Хотя программа *TSSAbloy* с рядом ограничений позволяет выполнять и эти функции.

3. Установка автономной системы

Для установки упрощенной версии СКУД с электронными ключами следует скопировать с дистрибутивного диска папку *TSS_Abloy* на жесткий диск ПК.

Далее следует:

- Установить службу обмена данными *TSSTransport* запуском командного файла *..\TSS_Abloy\Transport\Transport_install.bat* (выполняется с правами администратора).
- Стартовать *..\TSS_Abloy\TSSAbloy.exe* и начать работу по описанию и настройки системы, как указано в разделе Настройка подсистемы на контроллере

4. Установка подсистемы, как части СКУД

Далее речь пойдет об установке подсистемы управления электронными замками как части СКУД TSSProfi. При этом предполагается, что ПО СКУД уже установлено и корректно функционирует.

Установка выполняется копированием с дистрибутивного диска следующих данных:

- Всей папки *TSS_Abloy* на жесткий диск сетевого ПК.
- Содержимого папки *..\TSS_Abloy\ACS* в папку *..ACS* (т.е. в каталог с установленным ПО *TSSProfi*).

Далее следует:

- Установить службу взаимодействия *..\ACS\PSrvc_abloyTSS.exe* запуском командного файла *..\ACS\PSrvc_install.bat* (выполняется с правами администратора).
- Для автоматического старта службы при запуске СКУД и контроля ее работоспособности необходимо добавить в файл *ACS\AcsgmsServer.INI* содержимое файла *TSSAbloyInst/ACS/ToAcsgmsServerINI.txt* и рестартовать службу *AcsgmsServer*.
- Стартовать *..\TSS_Abloy\TSSAbloy.exe* и выполнить работу по описанию и настройки оборудования *Abloy*, как указано в разделе Настройка подсистемы на контроллере.
- Выполнить описание оборудования *Abloy* в ПО *Конфигуратор СКУД*.
- Перезапустить ядро СКУД и начать проверку работы системы в целом.

При обновлении подсистемы, достаточно скопировать только файл *PSrvc_abloyTSS.exe*, и то если дата его создания превышает дату создания прежнего. В этом случае, перед копированием файла *PSrvc_abloyTSS.exe* необходимо остановить службу, после копирования стартовать ее снова.

5. Настройка подсистемы на контроллере

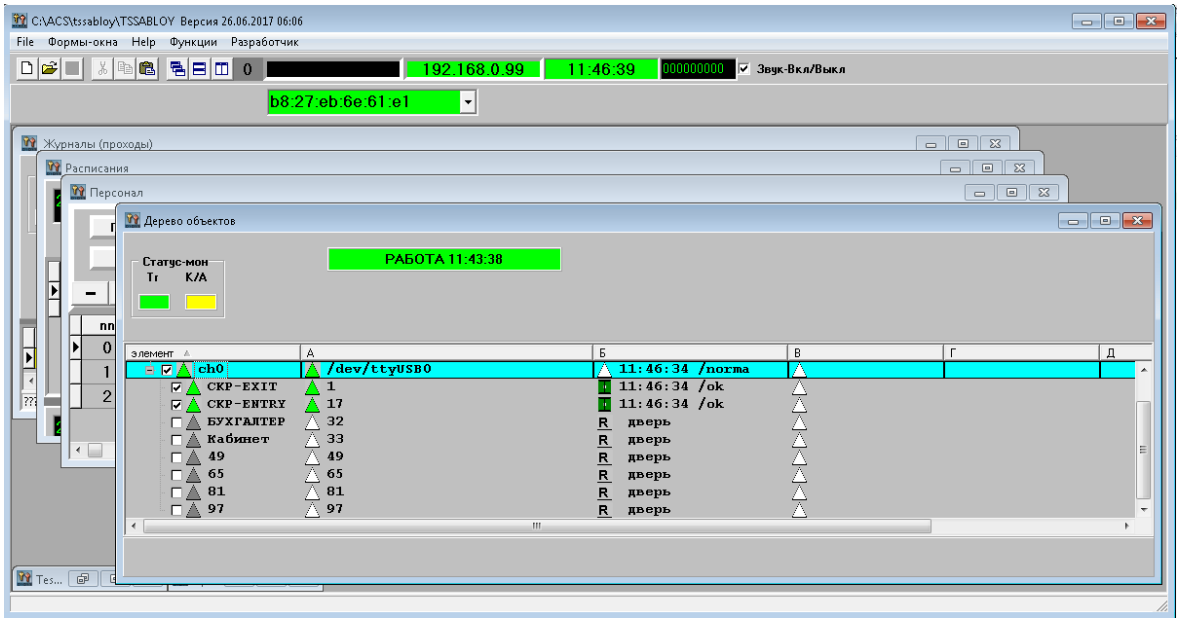
5.1. ПО управляющего контроллера

Конфигурирование автономной системы и диагностика ее работы выполняется на ПК под управлением ОС Windows в программе *TSSAbloy*. Эта же программа позволяет обеспечить настройку полноценной автономной системы контроля доступа, построенной на электронных замках, а именно:

- Ввод данных об электронных ключах сотрудников.
- Мониторинг работы.

Прочие возможности СКУД, такие как отображение информации в реальном времени, формирование отчетов и другие реализуются только при использовании ПО TSSProfi.

Программа *TSSAbloy* имеет многооконный интерфейс.



В числе основных окон следующие:

- Дерево объектов системы.
- Список персонала.
- Диагностические сообщения.
- Таблица расписаний.
- Журнал проходов.
- Таблица алгоритмов.

5.2. Подключение управляющего контроллера

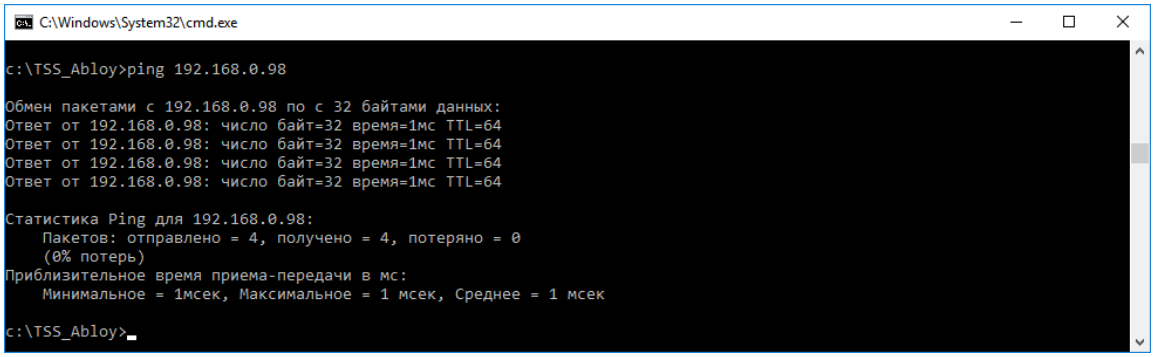
Управляющий контроллер *TSS2010-DV* является сетевым устройством с предустановленным собственным IP адресом, указанным в паспорте на изделие. По умолчанию – 192.168.0.90/24.

Для обеспечения доступа к контроллеру управляющих программ необходимо:

- Подключить его к службе *TSSTransport*, т.е. указать IP-адрес ПК Сервера СКУД.
- Изменить его IP-адрес в соответствии с адресацией ЛВС объекта.

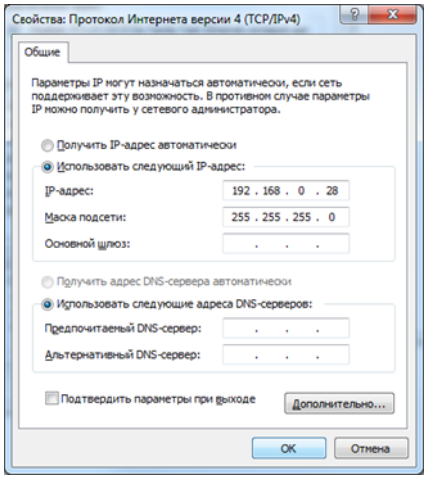
5.2.1. Подключение к Транспорту

Прежде всего, необходимо обеспечить доступ к контроллеру через ЛВС с ПК - либо через локальную сеть, либо напрямую. К дальнейшим шагам можно переходить только при положительном ответе команды *ping* (например, '*ping 192.168.0.90*'), как показано на рисунке.



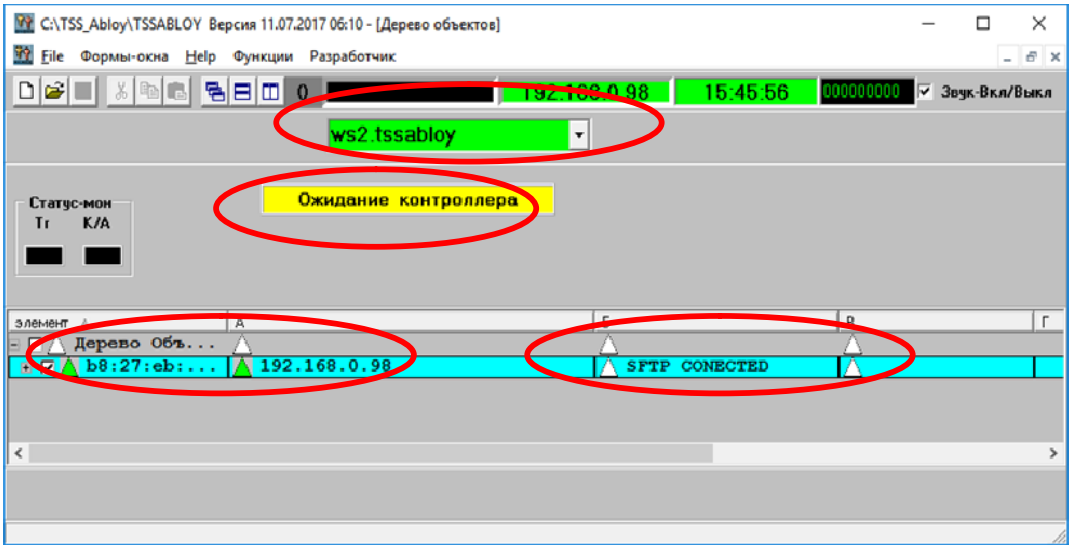
Если из рабочей сети не видно предустановленного IP адреса контроллера, следует:

- Изменить IP адрес сетевой карты ПК на любой в диапазоне 192.168.0.1 - 192.168.0.255 с помощью окон свойств сетевых соединений *Панели управления* Windows.
- Обеспечить прямое (или через свитч) подключение контроллера к ПК с ПО *TSSAbloy*.



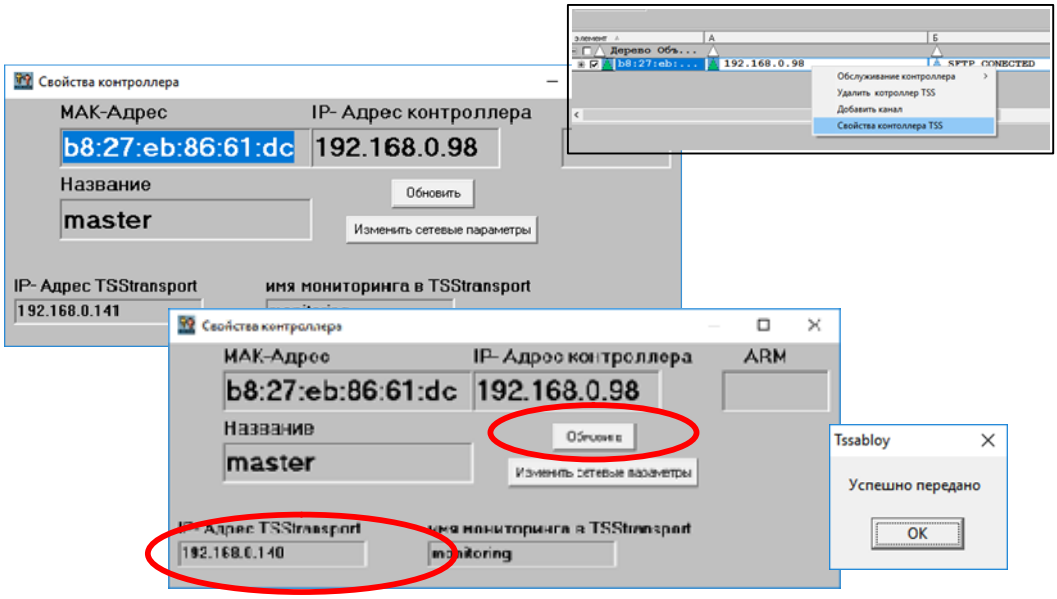
Дальнейшие действия выполняются с помощью программы *TSSAbloy*.

При указанном подключении контроллера после старта отобразится следующее окно (в данном примере заводской IP адрес – 192.168.0.98).



Обратите внимание на следующие особенности:

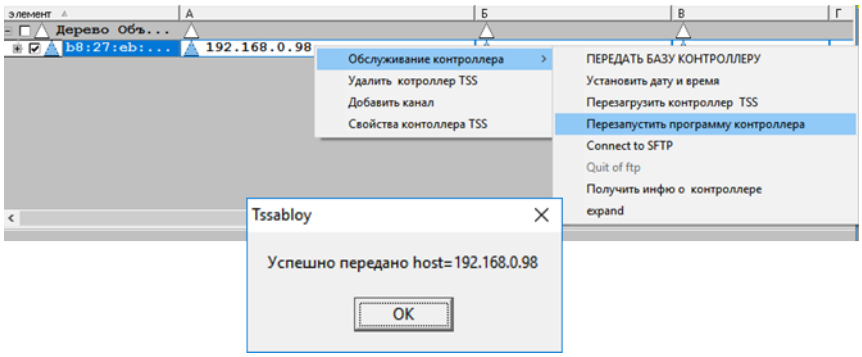
- В дереве объектов должен появиться контроллер, MAC- и IP адреса которого соответствуют его паспортным данным.
- В поле Е должно значится «SFTP connected» (т.е. установлено SFTP соединение, которое используется для первоначальной настройки).
- В окне присутствует транспарант желтого цвета с текстом *Ожидание контроллера*.
- В списке клиентов *Транспорта* отображается только один процесс – *TSSAbloy* с префиксом в виде имени ПК и точки.



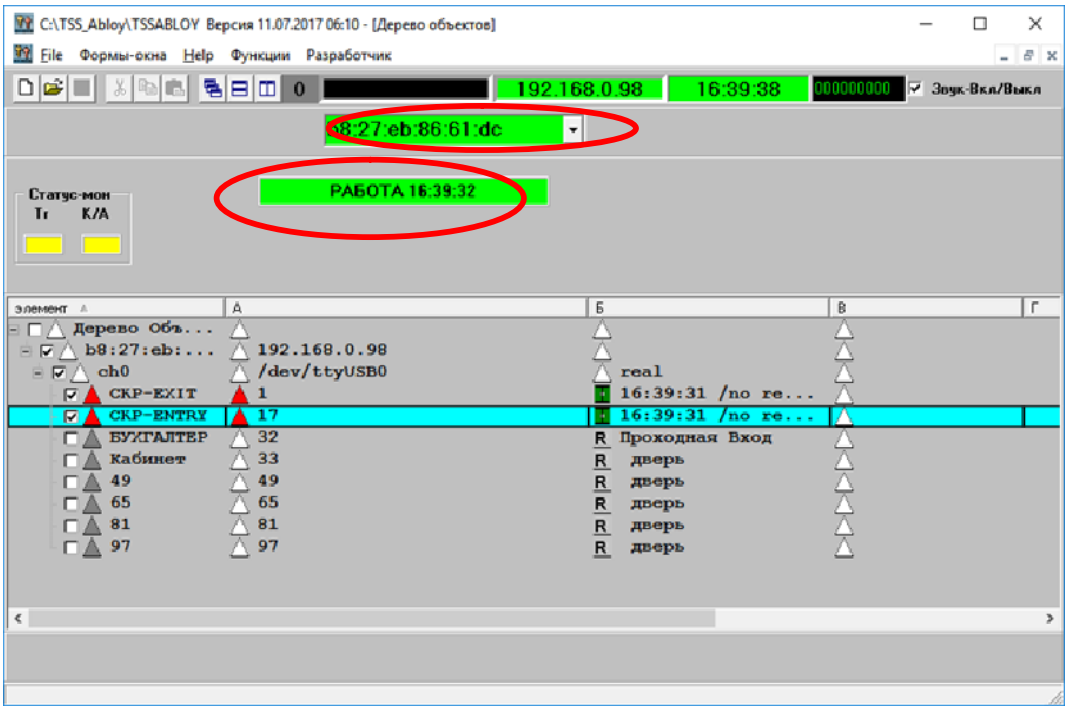
Из всплывающего меню на строке контроллера выбирается пункт *Свойства контроллера TSS* и в появившимся окне указывается IP адрес ПК, на котором установлен *Транспорт* системы. В данном случае это адрес текущего ПК.

Для сохранения и передачи изменений на контроллер следует нажать клавишу *Обновить*. Положительный результат подтверждается *сообщением Успешно передано*.

После нажатия ОК и возврата в окно дерева объектов необходимо выполнить перезагрузку программы контроллера. Это делается из контекстного меню выбором пунктов *Обслуживание контроллера – Перезапустить программу контроллера*.



После нажатия клавиши ОК и по окончанию перезапуска ПО контроллера последний зарегистрируется в *Транспорте* на данном ПК и система будет полностью готова к работе или настройки оборудования электронных замков.



5.2.2. Изменение IP адреса

Если диапазон адресов ЛВС не позволяет работать с предустановленным адресом контроллера, этот адрес (равно как и иные сетевые настройки) может быть изменен.

Операция выполняется в окне *Сетевые параметры* (смотрите рисунок).

Принцип изменения сетевых настроек заключается в редактировании конфигурационных Linux файлов.

Для редактирования содержимое файла надо считать, выбрав строку Interfaces и нажав клавишу *Поучить из контроллера*.

После подтверждения получения файла его содержимое отобразится в окне редактирования.

Далее следует изменить необходимые строковые параметры, сохранить (локально) и передать на контроллер одноименными клавишами.

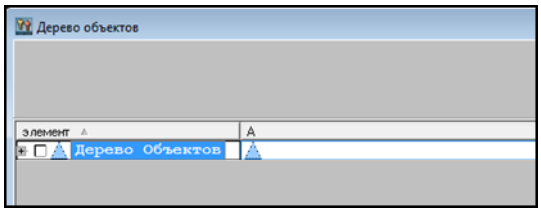
Для того чтобы изменение адреса вступило в силу следует перезагрузить контроллер из пункта вышеприведенного контекстного меню: *Обслуживание контроллера – Перезагрузить контроллер* или перезагрузить контроллер вручную.

После этого желательно сразу изменить IP адрес на новый, как описано выше (в окне Свойства контроллера).

Далее контроллер и ПК включаются в общую ЛВС, и перезапускается программа *TSSAbloy*.

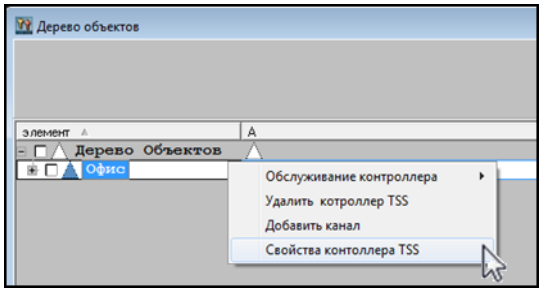
5.3. Конфигурирование системы на контроллере

5.3.1. Объекты



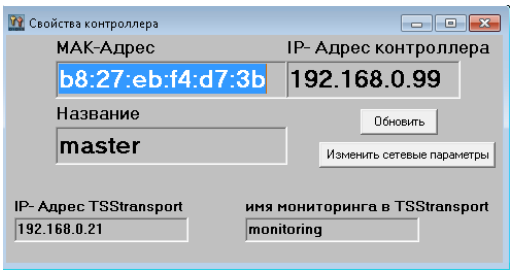
Конфигурирование системы выполняется в окне *Дерево объектов*.

Шаг 1



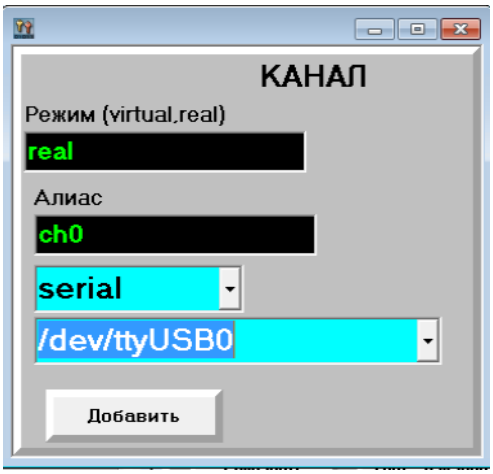
Первым шагом является создание управляющих контроллеров, к каждому из которых подсоединены «свои» хабы. Контроллер создается посредством единственного пункта всплывающего меню *Создать контроллер*.

Шаг 2



В меню созданного таким образом элемента дерева *Контроллер* следует выбрать пункт *Свойства контроллера TSS*. В окне свойств необходимо прописать MAK-адрес контроллера (из паспорта) и указать его произвольное имя.

Шаг 3



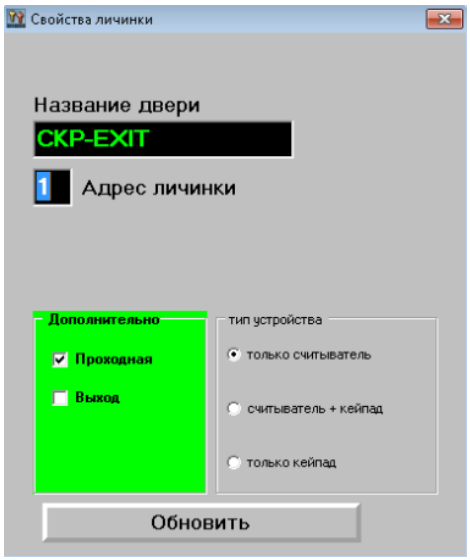
Для каждого контроллера системы создаются каналы через элемент меню *Добавить канал*.

В окне *Свойства канала* указываются:

- Тип используемого канала (помните, что речь идет об ОС контроллера, т.е. Linux):
  - Serial – USB-порт (с созданием логического COM-порта).
  - RS 485.
- Системное имя канала – выбирается из списка Linux устройств, соответствующих физическим USB портам.
- Произвольное имя (алиас).
- Режим работы канала – real (значение virtual используется для эмуляции работы электронных замков).

Шаг 4

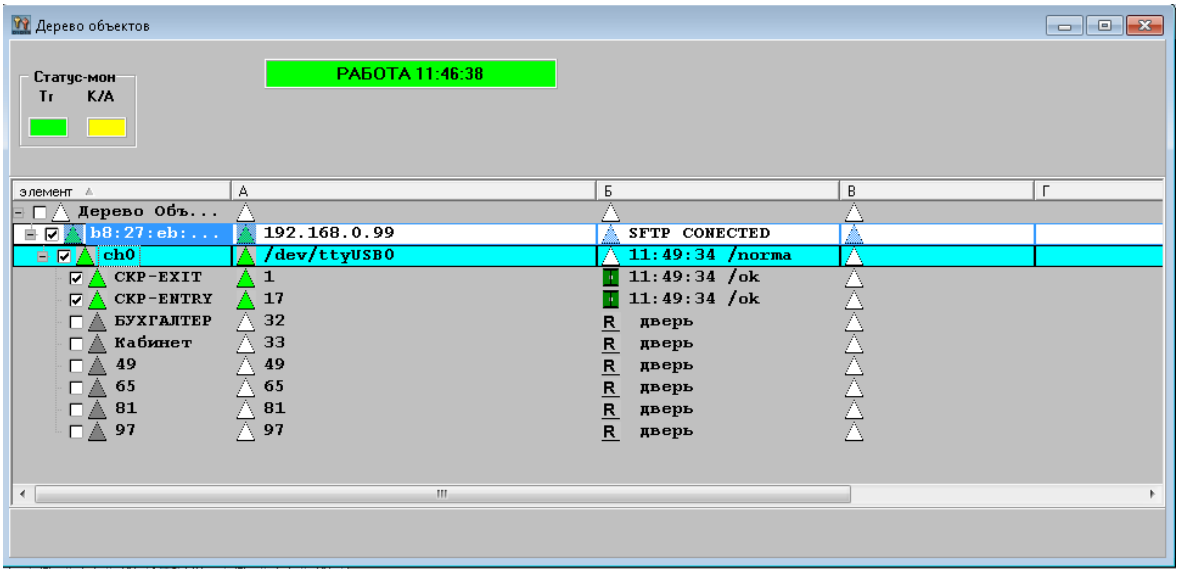
Для каждого канала создаются электронные замки (цилиндры, личинки) через элемент меню *Добавить личинку*.



В окне *Свойства личинки* указываются:

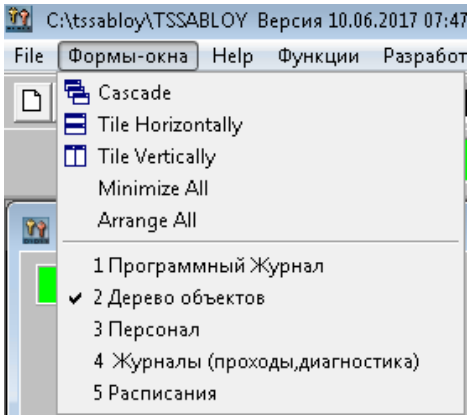
- *Адрес личинки* – адрес, под которым данная личинка зарегистрирована на одном из хабов.
- *Название двери* – произвольное имя (алиас).
- На панели *Дополнительно* устанавливаются дополнительные признаки данного пункта прохода:
  - *Проходная* – признак внешнего периметра, то есть что проход через дверь будет означать вход человека на территорию объекта или выход с него.
  - *Вход* – признак направления прохода: внутрь или наружу. Проходная обязательно является так называемой двухридерной дверью, то есть оснащенной отдельными считывателями на вход и на выход. Поэтому проходная будет состоять из двух личинок, одна из которых должная быть помечена, как *Вход*, другая – как *Выход*.
- На панели *тип устройства* указывается соответствующий параметр устройства считывания карт:
  - Только считыватель
  - Считыватель +кейпад
  - Только кейпад

В результате выполненного конфигурирования дерево объектов приобретет примерно такой вид:



5.3.2. Персонал

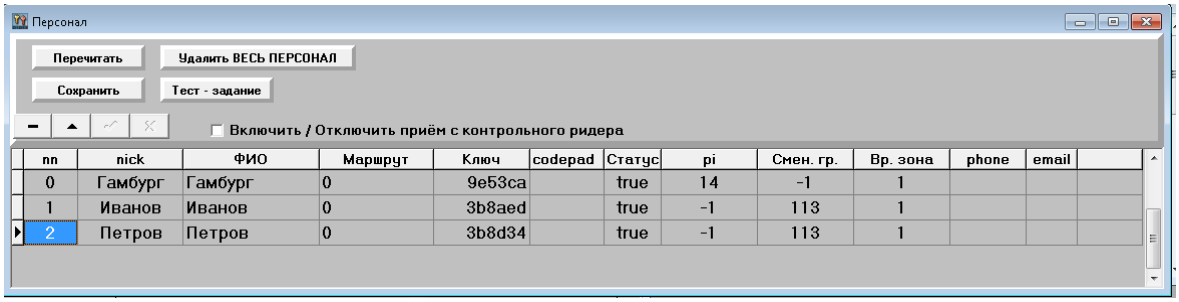
Как уже говорилось, система контроля доступа по электронным замкам может ботать как составная часть «большой» СКУД, в этом случае описанного выше конфигурирования достаточно для начала работы.



Однако, для автономного управления электронными замками в качестве самодостаточной системы, данная программа позволяет формировать список пользователей электронных ключей. Эту возможность рекомендуется использовать и для проверки корректности настройки системы.

Окно создания списка владельцев ключей (персонала) вызывается из *Главного меню* (*Формы-окна – Персонал*).

Окно *Персонал* представляет собой таблицу для построчного ввода данных и элементов навигации и управления данными. Непосредственно для принятия решений необходимы поля с кодом ключа, статусом, списком маршрутов и расписаний проходов[6].



nn	nick	ФИО	Маршрут	Ключ	codepad	Статус	pi	Смен. гр.	Вр. зона	phone	email
0	Гамбург	Гамбург	0	9e53ca		true	14	-1	1		
1	Иванов	Иванов	0	3b8aed		true	-1	113	1		
2	Петров	Петров	0	3b8d34		true	-1	113	1		

Код ключа заносится в поле *Ключ* либо вручную, либо с помощью контрольного считывателя[7].

Поле *Статус* (запрет на ключ) позволяет полностью блокировать ключ. Для разрешения доступа в этом поле должно стоять значение *True*.

Маршрутом называется совокупность пунктов прохода, в которые разрешен доступ владельцу данного ключа. Пункт прохода для данной системы – это адрес личинки, установленной на конкретной двери. Список доступных маршрутов – перечень адресов, разделенных запятой. Значение «0» означает проход везде. Маршруты прописываются в поле *Маршрут*.

Данные о **расписаниях**, то есть о временных ограничениях данного ключа хранятся в отдельных таблицах. Здесь же указываются ссылки на номера записи (точнее, на уникальные ID записи) соответствующих таблиц.

Всего имеется три вида расписаний[8]:

---

[6] Еще раз напомним, что при работе под управлением сервера СКУД вся информация о правах доступа заносится в базу данных автоматически.

[7] Смотрите раздел Регистрация кода ключа.

[8] Смотрите раздел Расписания.

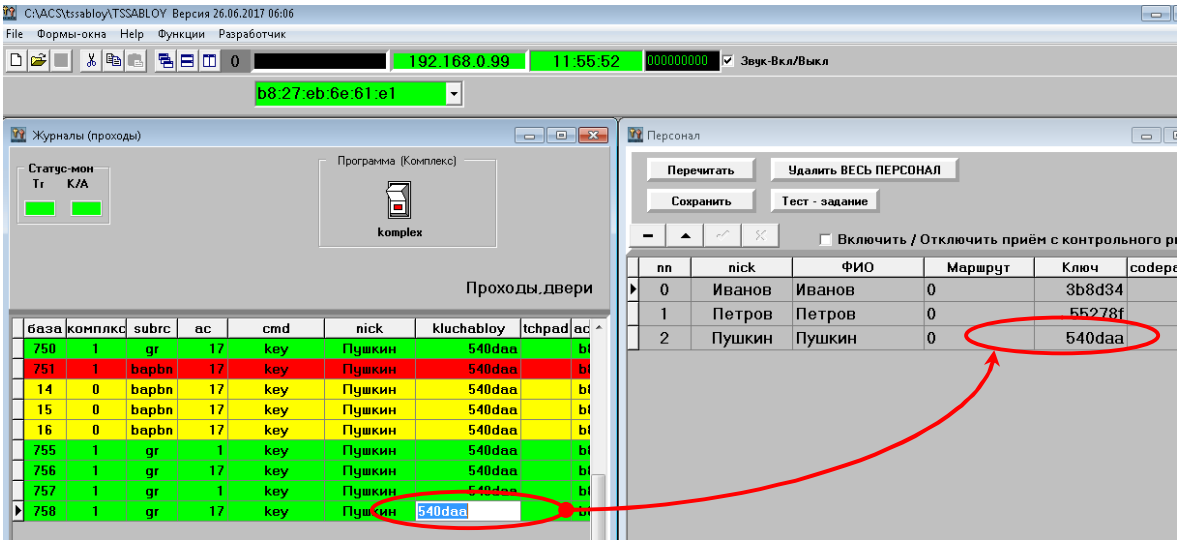
- Недельное расписание на каждый день недели (*временные зоны*). Ссылка на соответствующую запись хранится в поле *Вр. зона*.
- Сменные графики – плавающее расписание на каждый календарный день. Ссылка – в поле *Смен. гр.*
- Индивидуальные графики – исключения для отдельных работников на конкретные дни. Ссылка – в поле *pi*. На самом деле Pi – это уникальный номер человека в базе данных сотрудников, индивидуальные графики (в отличие от остальных) привязаны именно к нему.

5.3.3. Регистрация кода ключа

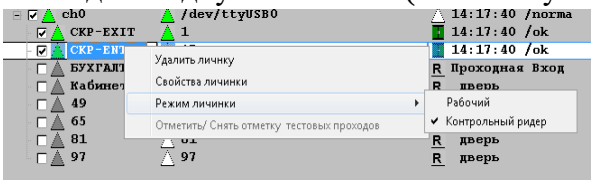
Перед тем, как начать заносить коды ключей в базу, необходимо включить тумблер в положение *komplex* на панели *Программа (Комплекс)* в окне *Журналы (проходы)*. Он загорится зеленым цветом и в нижней части окна начнут отображаться события. После этого можно приступать к занесению кодов ключей в базу данных.

Код ключа может быть занесен двумя способами[9]: вручную и посредством контрольного считывателя.

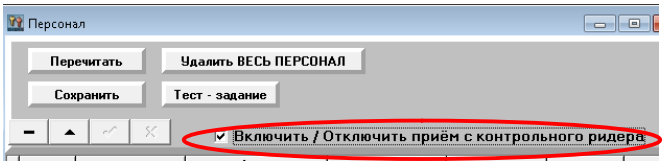
Для ручного занесения кода в поле *KluchAbloy* достаточно открыть окно проходов, приложить карту к любой личинке и скопировать полученный код, как показано на рисунке.



Для автоматического занесения ключа необходимо одну из личинок (ближайшую к столу оператора программы) описать, как контрольный считыватель. Данная операция выполняется в дереве объектов для соответствующего считывателя (смотрите рисунок).



Далее, в окне *Персонал* включить опцию *Включить приём с контрольного ридера*. После чего, код карты, поднесенной к данной личинке, пропишется в поле кода ключа текущей



[9] Не считая, конечно, его автоматическое занесение сервером СКУД.

записи. Для записи следующего ключа необходимо создать новую строку клавишей *стрелка вниз* на клавиатуре.

Обратите внимание, что для работы контроллера в составе ПО СКУД TSS все считыватели Abloy должны быть описаны как рабочие, чтобы исключить возможные несоответствия в работе программы контроллера и ПО СКУД TSS.

5.3.4. Маршруты

Маршрут – это перечень пунктов прохода, в которые данному лицу разрешен доступ. Поскольку пунктом прохода в данной системе является дверь, оборудованная электронным замком, то номер этой двери в списке маршрутов соответствует адресу конкретной личинки. Направление перемещения значения не имеет.

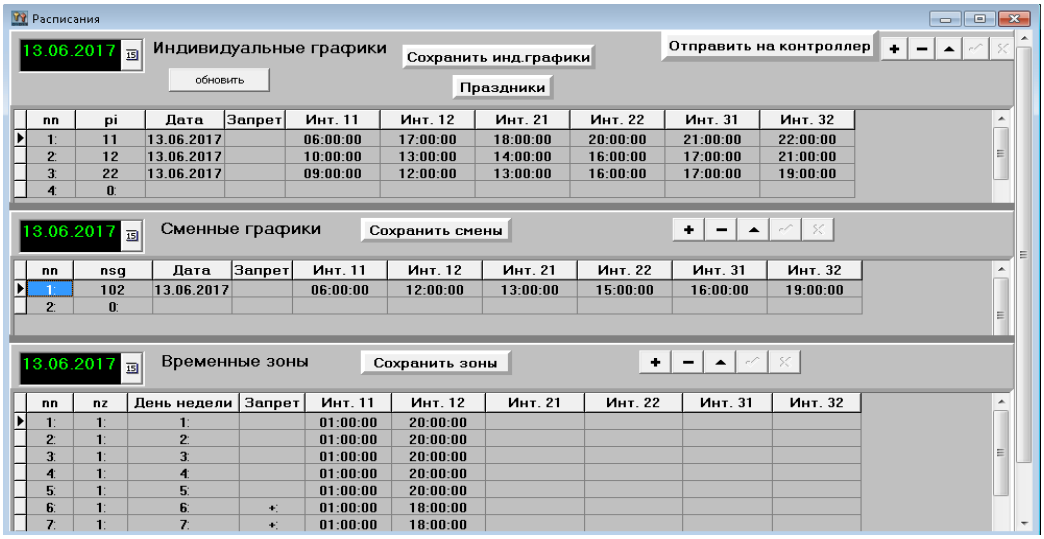
Разрешенные для прохода адреса заносятся в записи сотрудника в поле *Marsrut* через запятую. Значение «0» означает доступ во все помещения. Значение «-1» – полный запрет доступа.

5.3.5. Расписания

Три вида расписаний обрабатываются в порядке следующей приоритетности:

- Индивидуальные графики – исключения для отдельных работников на конкретные дни.
- Сменные графики – плавающее расписание на каждый календарный день.
- Понедельное расписание на каждый день недели (*временные зоны*).

Таблицы выглядят примерно следующим образом:



Индивидуальные графики действуют только на конкретную дату. В случае совпадения текущего числа с заданным, проверяются все три разрешенных для прохода интервала времени. Если в поле *Запрет* стоит +, проход запрещается.

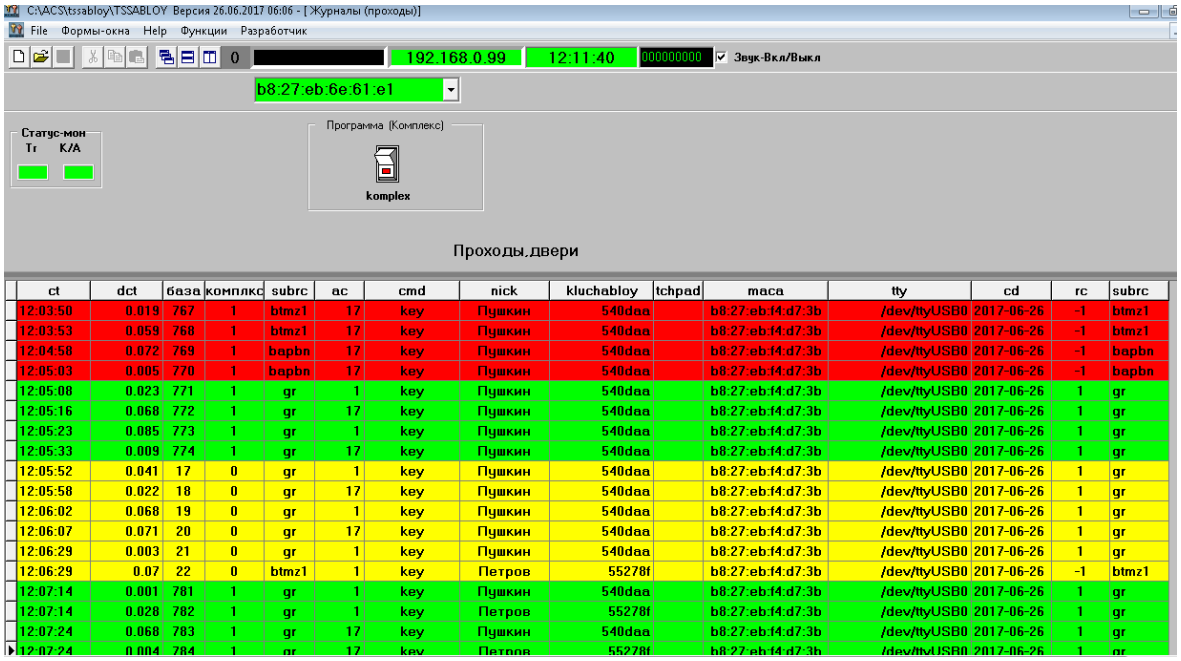
Если у сотрудника указан номер сменного графика, то производится контроль по таблице смен. При отсутствии записи с данным номером проход запрещается. При наличии – выполняются все указанные выше проверки. Признаком отсутствия у персоны сменного графика является значение поля *nsg -1*.

В случае отсутствия запретов или разрешений по верхним графикам, проверяется расписание по дням недели. Для прохода необходима совокупность признаков: на-

личие записи в таблице с индексом *nz*, совпадение с текущим днем недели, попадание текущего времени в один из разрешенных интервалов.

Отметим, что задание временн*ы*х ограничений в программе TSSAbloy имеет смысл только для работы подсистемы в автономном режиме, либо для тестовых проверок. При работе в составе ПО верхнего уровня расписания создаются средствами ПО СКУД TSS Profi, прежде всего программой Персонал.

5.3.6. Журналы (проходы)



ct	dct	база	комплкс	subrc	ac	cmd	nick	kluchabloy	tchpad	maca	tty	cd	rc	subrc
12:03:50	0.019	767	1	btmz1	17	key	Пушкин	540daa		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	-1	btmz1
12:03:53	0.059	768	1	btmz1	17	key	Пушкин	540daa		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	-1	btmz1
12:04:58	0.072	769	1	bapbn	17	key	Пушкин	540daa		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	-1	bapbn
12:05:03	0.005	770	1	bapbn	17	key	Пушкин	540daa		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	-1	bapbn
12:05:08	0.023	771	1	gr	1	key	Пушкин	540daa		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	1	gr
12:05:16	0.068	772	1	gr	17	key	Пушкин	540daa		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	1	gr
12:05:23	0.085	773	1	gr	1	key	Пушкин	540daa		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	1	gr
12:05:33	0.009	774	1	gr	17	key	Пушкин	540daa		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	1	gr
12:05:52	0.041	17	0	gr	1	key	Пушкин	540daa		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	1	gr
12:05:58	0.022	18	0	gr	17	key	Пушкин	540daa		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	1	gr
12:06:02	0.068	19	0	gr	1	key	Пушкин	540daa		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	1	gr
12:06:07	0.071	20	0	gr	17	key	Пушкин	540daa		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	1	gr
12:06:29	0.003	21	0	gr	1	key	Пушкин	540daa		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	1	gr
12:06:29	0.07	22	0	btmz1	1	key	Петров	55278f		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	-1	btmz1
12:07:14	0.001	781	1	gr	1	key	Пушкин	540daa		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	1	gr
12:07:14	0.028	782	1	gr	1	key	Петров	55278f		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	1	gr
12:07:24	0.068	783	1	gr	17	key	Пушкин	540daa		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	1	gr
12:07:24	0.004	784	1	gr	17	key	Петров	55278f		b8:27:eb:f4:d7:3b	/dev/ttyUSB0	2017-06-26	1	gr

В окне Журналы отображаются сообщения от считывателей. Желтым цветом выделяются автономные сообщения, красным – запрет прохода, зеленым – разрешения на проход. Для того чтобы сообщения начали поступать, необходимо на панели Программа (Комплекс) включить тумблер в положение *komplex*.

При наличии автономных событий в контроллере они появятся в окне, выделенные желтым цветом. Комплексные события будут появляться по мере проходов.

В поле *subrc* отмечается решение системы по правам доступа.

При разрешении прохода указывается gr (granted). При этом строка выделяется зеленым.

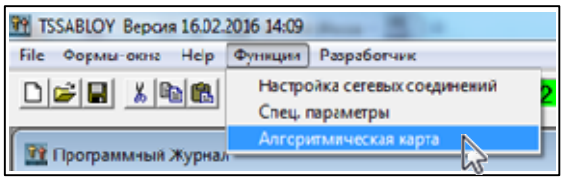
При запрете прохода строка помечается красным и заносится одна из следующих причин запрета:

- bs – запрет по статусу (поле *статус* в окне *Персонал*)
- bapbn – запрет по антипассбэку
- nf – ключ неизвестный
- btmz1 – запрет по индивидуальному графику (поле *pi* в окне *Персонал*)
- btmz2 – запрет по сменному графику (поле *смен. гр.*)
- btmz3 – запрет по временной зоне (поле *вр. зона*)
- bm – запрет по маршруту (поле *маршрут*)

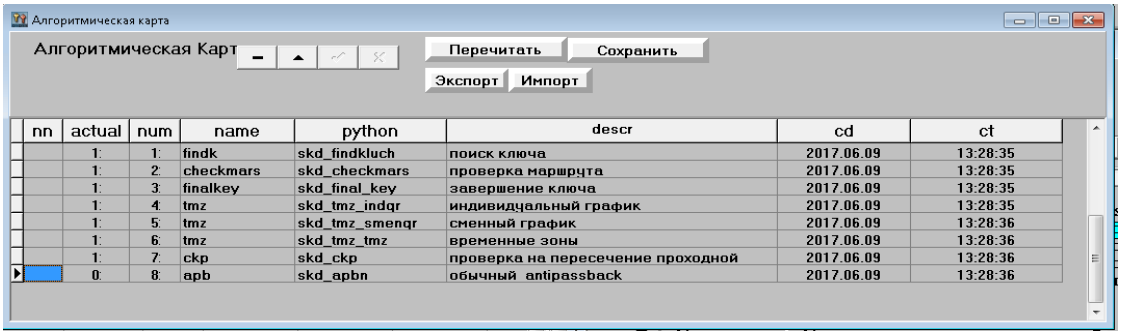
5.4. Глобальные режимы контроля доступа

В системе действуют следующие алгоритмы контроля доступа:

- Код ключа.
- Запрет на ключ.
- Срок действия ключа.
- Антипасбэк (запрет повторного прохода).
- Проходная (запрет прохода во внутренние помещения без пересечения периметра).
- Маршруты.
- Расписания.



Управлять алгоритмами можно в окне *Алгоритмическая карта*. В представленной там таблице расположены все перечисленные алгоритмы. Часть полей таблицы являются служебными, редактировать допускается только поля *Actual* и *Num*.



nn	actual	num	name	python	descr	cd	ct
	1	1	findk	skd_findkluch	поиск ключа	2017.06.09	13:28:35
	1	2	checkmars	skd_checkmars	проверка маршрута	2017.06.09	13:28:35
	1	3	finalkey	skd_final_key	завершение ключа	2017.06.09	13:28:35
	1	4	tmz	skd_tmz_indqr	индивидуальный график	2017.06.09	13:28:35
	1	5	tmz	skd_tmz_smenqr	сменный график	2017.06.09	13:28:36
	1	6	tmz	skd_tmz_tmz	временные зоны	2017.06.09	13:28:36
	1	7	ckp	skd_ckp	проверка на пересечение проходной	2017.06.09	13:28:36
	0	8	apb	skd_apbn	обычный antipassback	2017.06.09	13:28:36

Поле *Actual* позволяет выключать из процесса принятия решения те или иные алгоритмы. Для этого следует поставить 0 и сохранить таблицу, затем перезапустить программу контроллера, чтобы изменения вступили в силу.

Последовательность исполнения алгоритмов (или приоритетность) задается нумерацией в колонке *Num*. При необходимости эта последовательность может быть изменена.

Клавиша *Импорт* позволяет загрузить новые алгоритмы «от производителя», для чего файл *algsexport.txt* должен быть помещен в папку *TSSAbloy*.

6. Конфигурирование подсистемы на Сервере

Включение беспроводных замков *Abloy-Aperio* в состав СКУД выполняется стандартными средствами ПО TSS2000 Profi.

Предполагается, что читатель данного раздела хорошо знаком с логикой работы и системой настроек СКУД марки TSS. Поэтому здесь будут освещены только вопросы, касающиеся работы с подсистемой беспроводных замков.

6.1. Подготовительные работы

Перед конфигурированием Сервера СКУД необходимо выполнить описанные в предыдущих разделах процедуры подключения оборудования и конфигурирования управляющего контроллера. На момент начала работ в *Конфигураторе* СКУД работоспособность подсистемы должна быть протестирована в автономном режиме и подготовлен список адресов электронных личинок.

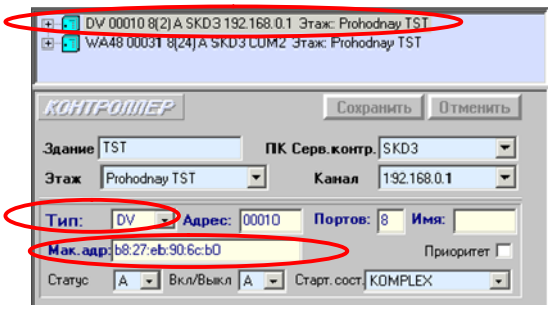
6.2. Логика работы

Работе в единой программной среде СКУД обеспечивает двунаправленный обмен данными между управляющими контроллерами TSS-Abloy и ПО СКУД в режиме реального времени. **Еще раз подчеркнем, что управление электронными замками осуществляется непосредственно контроллерами TSS-Abloy, независимо от наличия связи с Сервером и ПО СКУД.**

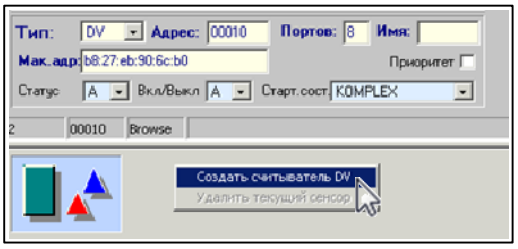
Обмен данными позволяет, с одной стороны, актуализировать все изменения, выполненные в СКУД по занесению и изменению данных о владельцах ключей (коды карт, права доступа) в контроллерах TSS-Abloy, а с другой – передавать информацию о перемещении лиц в пространстве, оснащенным беспроводными замками, в комплекс СКУД для отображения данных о проходах и записи их в *Системный журнал*.

6.3. Настройка

Настройка выполняется в программе *Конфигуратор*.



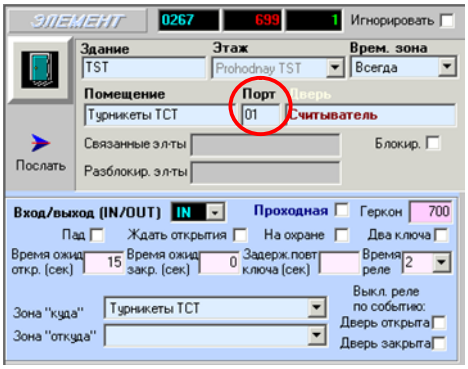
Для управляющего системой электронных замков контроллера должно быть создано описание тем же способом, что и для обычных контроллеров СКУД. При этом тип контроллера должен быть выбран DV и указан его MAC-адрес.



Далее должны быть созданы элементы контроллера – непосредственно электронные замки, являющиеся с точки зрения СКУД обычными считывателями. Для контроллера DV они создаются на панели элементов посредством контекстного меню, как показано на рисунке.

Описание считывателя DV отличается от описания обычных считывателей СКУД тем, что каждый из них имеет собственный адрес. Этот адрес задается в поле *Порт*.

Обратите внимание, что далеко не все мы, действующие для обычных считывателей СКУД, работают на электронных замках. Это зависит как от типа самих считывателей, так и от версии ПО.



7. Работа

После настройки системы электронные замки становятся такими же элементами СКУД, как и стандартные считыватели, и управление ими и отображение их работы производится по общим правилам.

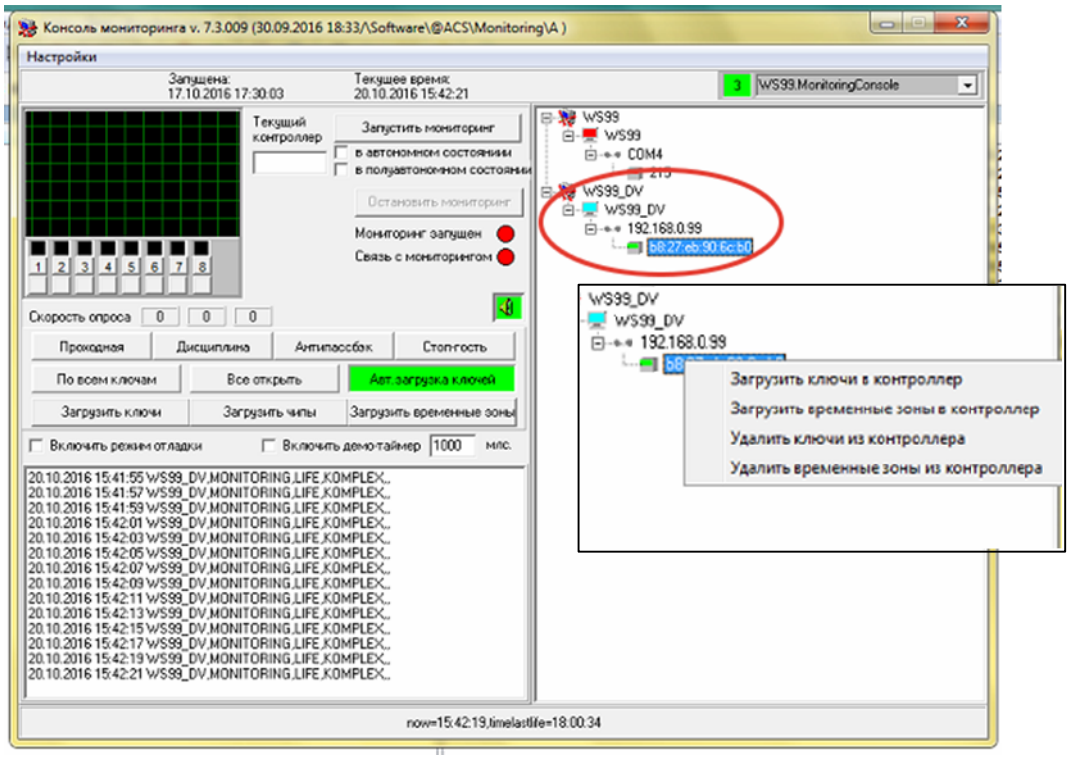
Так, любое действие с карточкой сотрудника в программе *Бюро пропусков* (добавление, удаление, изменение прав доступа) делает эти действия актуальными и для электронных замков.

Для работы системы глобальных запретов (например, режима *проходная*) выполняется синхронизация всей базы персонала, независимо от того, имеет ли персона права прохода по электронным замкам.

Любое событие, произошедшее на этих замках (проход, запрет прохода), отображается в клиентских приложениях СКУД.

Эти события участвуют в формировании различных отчетов (проходы, нарушения, рабочее время).

При правильном конфигурировании в *Консоли Мониторинга* контроллер управления электронными замками будет отображаться следующим образом:



Загрузка данных в контроллер выполняется посредством контекстного меню.

Напоминаем, что если база ключей не загружена в управляющий контроллер, то система электронных замков работать не будет, даже, если СКУД функционирует в комплексном режиме. То же относиться и к расписаниям.

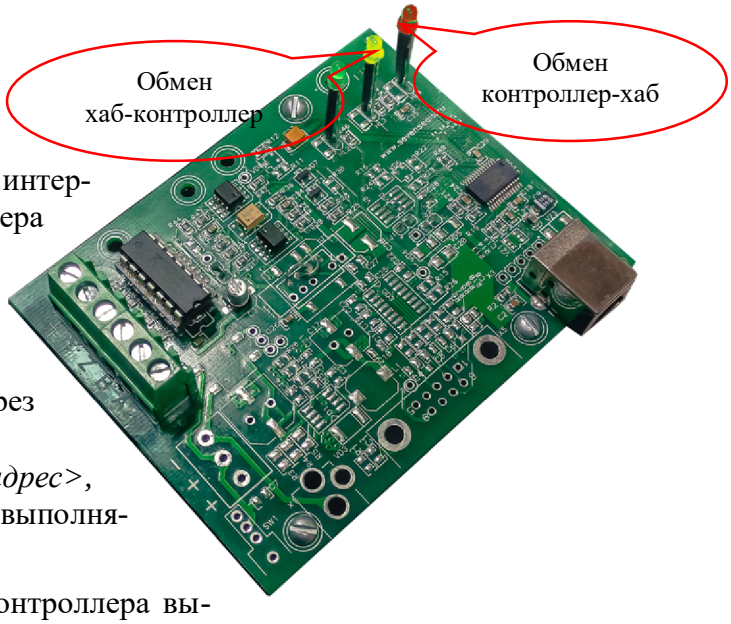
8. Средства диагностики

Данная глава предназначена только для опытных пользователей Windows.

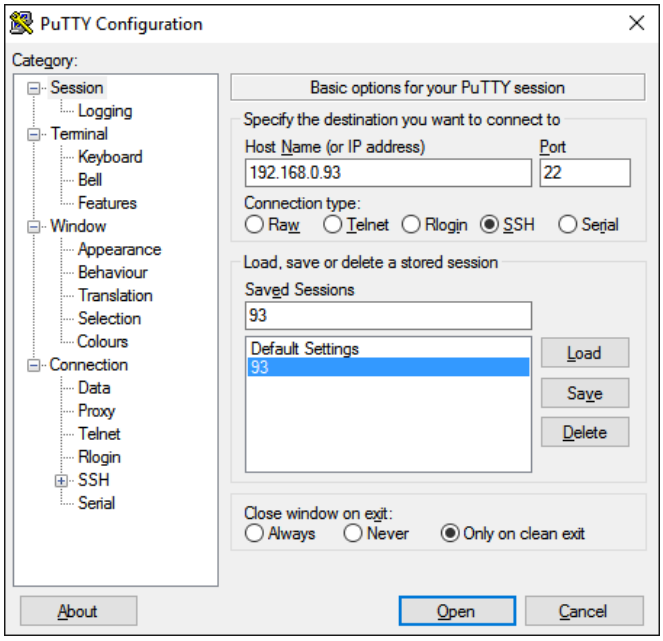
В случае неработоспособности подсистемы следует придерживаться следующей последовательности диагностирования.

Проверка корректности физических соединений:

- Линия замки – хаб:
  - Наличие питания на хабе.
  - Корректная индикация на хабе при прикладывании карты к электронному замку. При отсутствии индикации следует выполнить операции *unpair* и *pair*.
- Хаб–контроллер:
  - Корректная индикация на хабе связи с системой управления (EAC).
  - Корректная индикация на интерфейсной плате контроллера (смотрите рисунок).
- Линия контроллер-компьютер:
  - Физическое подключение через ЛВС.
  - Успешная команда *ping<IP адрес>, например: ping 192.168.0.99* (выполняется из командной строки).



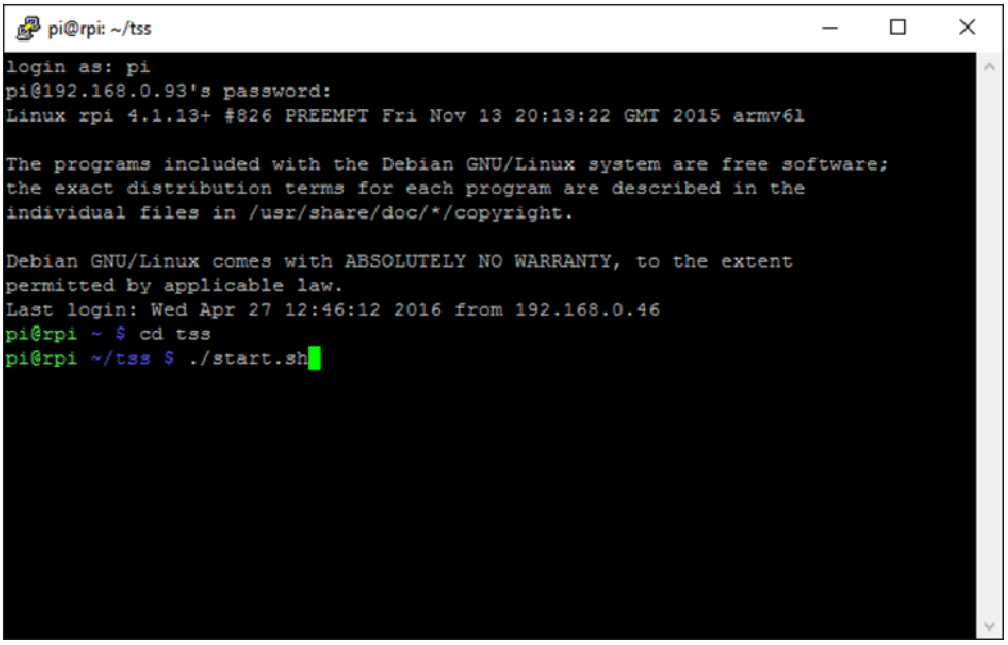
Дальнейшая диагностика работы контроллера выполняется из окна Linux консоли, организованной, например, прилагаемой к дистрибутиву утилитой PUTTY. Примерная настройка соединения показана на рисунке.



Заметьте, что скорость установления соединения зависит от способа подключения: при прямом соединении контроллер - компьютер она ниже.

Логин для открытия сессии *pi*, пароль *r*.

Как стартовать (рестартовать) ПО контроллера показано на рисунке.



Другие полезные команды:

Ifconfig – посмотреть сетевые настройки.

Sudo reboot– перезагрузка контроллера.