ИСО «Орион»

Биометрический контроллер доступа

C2000-BIOAccess-MA300

Руководство пользователя

Настоящее руководство пользователя предназначено для изучения принципов работы и эксплуатации биометрического контроллера доступа «С2000-BIOAccess-MA300».

Пожалуйста, внимательно ознакомьтесь с изложенными в руководстве инструкциями, перед тем как подключать, настраивать, эксплуатировать или обслуживать контроллер.

В данном руководстве используются следующие термины:

аутентификация – процедура проверки подлинности пользователя;

верификация – проверка предоставленного идентификатора на соответствие записанному в базу данных;

верификация отпечатка пальца - подтверждение соответствия отпечатка пальца заданному шаблону.

идентификатор – уникальный признак пользователя (номер, Proximity-карта, отпечаток пальца).

СКУД – система контроля и управления доступом.

ПК – персональный компьютер.

Содержание

1 Общие сведения 4
1.1 Меры предосторожности 5
1.2 Получение качественных изображений отпечатков пальцев 5
2 Основные сведения о контроллере 6
2.1 Внешний вид, органы управления 6
2.2 Основные технические данные 7
2.3 Комплект поставки 8
3 Установка и подключение контроллера 8
3.1 Монтаж контроллера 8
3.2 Схемы электрических соединений 9
3.3 Подключение к контроллеру периферийного оборудования 10
3.4 Подключение к ПК 12
4 Базовая настройка контроллера 13
4.1 Автономная работа 13
4.1.1 Настройка контроллера в BAProg 13
4.1.2 Добавление пользователей и временных окон 17
4.2 Работа контроллера в составе АРМ «Орион Про» 21
5 Обслуживание 22
6 Гарантии изготовителя (поставщика) 22
7 Сведения о сертификации 22
Приложение 1 23
Приложение 2 28

1 Общие сведения

Биометрический контроллер доступа «С2000-BIOAccess-MA300» (далее – контроллер) предназначен для организации системы контроля и управления доступом (СКУД) по биометрическим идентификаторам – отпечаткам пальцев и Proximity-картам.

Контроллер может работать автономно и совместно с АРМ «Орион Про».

Контроллер оснащён оптическим сканером отпечатков пальцев и встроенным считывателем Proximity-карт стандарта EM-Marine.

В контроллере предусмотрен режим мульти-идентификации – предоставление доступа по комбинации двух идентификаторов (отпечаток пальца и Proximity-карта).

Решение о предоставлении доступа на охраняемую территорию принимается контроллером и основывается на правах доступа и временных окнах.

Контроллер обеспечивает световую и звуковую индикацию своего состояния.

Контроллер оснащён реле типа «сухой контакт» на переключение, а также входами для подключения датчика двери и кнопки выхода. Кроме того, в контроллере предусмотрены контакты для управления сиреной.

Контроллер оборудован датчиком вскрытия корпуса.

Для хранения значений конфигурационных параметров контроллера, информации о пользователях и журналов событий используется энергонезависимая память.

Настройка контроллера «С2000-BIOAccess-MA300» для автономной работы выполняется с помощью программы BAProg. Новейшую версию программы BAProg можно скачать с сайта компании «Болид» http://bolid.ru/production/orion/po-orion/baprog.html.

Электропитание контроллера осуществляется от источника постоянного тока напряжением 12 В. В качестве источника питания рекомендуется применять «РИП-12» производства компании «Болид».

Контроллер предназначен для установки внутри помещений, в том числе неотапливаемых, защищённых от ударных воздействий, и рассчитан на непрерывную круглосуточную работу. Корпус контроллера допускает падание брызг воды в любом направлении (степень защиты оболочки IP54).

Контроллер относится к невосстанавливаемым, периодически обслуживаемым изделиям.

1.1 Меры предосторожности

Не устанавливайте и не используйте контроллер в условиях очень яркого освещения. Яркий свет нарушает способность считывателя получать чёткие отпечатки пальцев.

Диапазон рабочих температур контроллера: от минус 10 до плюс 60 ºС. Не подвергайте контроллер воздействию источников тепла.

При использовании контроллера отсутствует риск получения несанкционированного доступа к персональной информации, так как в памяти контроллера сохраняются не отсканированные изображения отпечатков пальцев, а только шаблоны отпечатков. При этом на основе шаблонов нельзя восстановить оригинальные изображения отпечатков пальцев.

Начиная с версии Ver 6.60 Jul 20 2016 в контроллере предусмотрена процедура сброса сетевых настроек. Процедура сброса описана в п.4.1.1 настоящего руководства.

Для предыдущих версий сброс возможен только в сервисном центре ЗАО НВП «Болид». При этом вся информация будет удалена из памяти контроллера.

1.2 Получение качественных изображений отпечатков пальцев

Качество получаемого изображения отпечатка пальца зависит от количества характерных особенностей рисунка кожи. Для пользователей, у которых отпечатки пальцев не обладают необходимым количеством характерных особенностей для однозначного результата аутентификации, рекомендуется регистрировать Proximity-карты.

Алгоритм получения отпечатка пальца позволяет выявить характерные особенности даже при не очень качественном изображении. Тем не менее, позиционирование пальца, а также влажность кожи и оказываемое на поверхность давление, являются важными факторами при получении качественного изображения отпечатка пальца.

Для получения качественного изображения отпечатка пальца необходимо удерживать палец у считывателя в течение двух секунд до получения отклика от контроллера. Палец нужно располагать в центре поверхности сенсора параллельно поверхности.

Правильное расположение пальца:

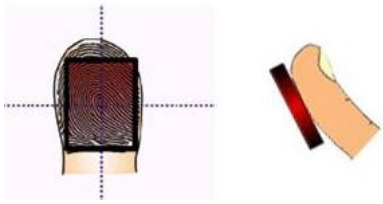


Рисунок 1. Правильное положение пальца при сканировании

2 Основные сведения о контроллере

2.1 Внешний вид, органы управления

Рисунок 2. Лицевая панель С2000-BIOAccess-MA300

На лицевой панели контроллера находятся (см. рис. 2):

1) светодиодный индикатор;
2) считыватель Proximity-карт стандарта EM-Marine;
3) считыватель отпечатков пальцев.

Светодиодный индикатор работает в нескольких режимах, перечисленных в таблице 1:

Таблица 1. Режимы работы светодиодного индикатора

Режим работы индикатора	Состояние контроллера
Выключен (после подачи питания)	Загружается операционная система контроллера
Мигает зелёный светодиод с частотой 0,5 Гц	Рабочее состояние
Включен зеленый	Идёт процесс верификации или программирования прибора
Загорается красный светодиод на 1с	Ошибка аутентификации
Загорается зелёный светодиод на 1с	Успешная верификация

С нижней стороны контроллера находится кнопка «Reset», позволяющая перезагрузить контроллер. Здесь же находятся разъём для подключения USB-накопителя (через переходник MiniUSB-USB, входящий в комплект поставки) и громкоговоритель.

С тыльной стороны контроллера выведены соединительные провода с разъёмами, ответные части разъемов входят в комплект поставки.

Контроль вскрытия прибора (отрыва от стены) реализован с помощью магнитного датчика, магнит закреплен на кронштейне прибора.

2.2 Основные технические данные

- Напряжение питания, В — от 9,6 до 14,4
- Потребляемый ток, А — не более 1
- Максимальное коммутируемое напряжение реле постоянное, В — 36
- Максимальный коммутируемый ток реле, А — 2
- Вероятность несанкционированного доступа, % — не более 0,0001
- Вероятность ложного задержания, % — не более 1
- Память контроллера, шаблонов отпечатков пальца — 1500
- Память контроллера, кодов Proximity-карт — 5000
- Объём буфера событий, записей — 100 000
- Диапазон температур, ºС — от минус 10 до плюс 60
- Относительная влажность воздуха, % — от 10 до 90
- Габаритные размеры, мм — 73×148×34,5
- Масса, кг — 1
- Степень защиты оболочки — IP54

2.3 Комплект поставки

В комплект поставки «С2000-BIOAccess-MA300» входят:

- «С2000-BIOAccess-MA300» – 1 шт.
- Паспорт – 1 экз.
- Инструкция по монтажу – 1 экз.
- Шаблон разметки для монтажа – 1 шт.
- Провода с разъёмами – 3 шт.
- Переходник MiniUSB-USB – 1 шт.
- Кронштейн – 1 шт.
- Винт для фиксации на кронштейне – 2 шт.
- Шуруп для крепления кронштейна – 4 шт.
- Отвёртка «звёздочка» Т10 – 1 шт.
- Диод FR 107 – 1 шт.
- DVD-диск с ПО – 1 шт.
- Proximity-карта (или брелок) стандарта EM-Marine – 1 шт.

3 Установка и подключение контроллера

3.1 Монтаж контроллера

Контроллер крепится к стене с помощью кронштейна. Для удобства монтажа в комплект поставки входит самоклеющийся прозрачный шаблон разметки. Для монтажа следует отсоединить кронштейн от контроллера. Для этого необходимо открутить винт в нижней части контроллера с помощью отвёртки из комплекта поставки, аккуратно потянуть кронштейн на себя и вверх. Кронштейн закрепляется на стене с помощью четырёх шурупов, провода выводятся через отверстие. После подключения всех требуемых электрических цепей и проверки работоспособности контроллер следует закрепить на кронштейне, зафиксировав его ранее открученными винтами.

Для закрепления контроллера на кронштейне используются винты под отвёртку Т10 «звёздочка», что является одним из способов защиты от несанкционированного доступа. Во избежание возможности несанкционированного доступа рекомендуется использовать винты из комплекта поставки.

По окончании монтажных работ следует удалить защитную плёнку со сканера отпечатков пальцев.

3.2 Схемы электрических соединений

Для подключения электрических цепей контроллера с тыльной стороны контроллера выведены провода с разъемами. Провода с ответными частями данных разъёмов входят в комплект поставки. Разъем RJ45 для подключения по Ethernet установлен непосредственно на провод, выведенный из контроллера. Во избежание неправильного подключения все разъёмы имеют разную форму. Для удобства подключения провода сгруппированы по назначению (контакты замка, сирены и пр.) и промаркированы соответствующим образом.

Разъем питания – однорядный разъем;

Основной разъем – двухрядный разъём;

Разъем Ethernet – стандартный разъём RJ45;

Разъем Wiegand – однорядный разъём.

Таблица 2. Назначение и описание контактов разъёма питания

Номер контакта	Название	Назначение, цвет подсоединяемого провода
1	+12V	Питание +12 В, красный
2	GND	Питание GND, черный

Таблица 3. Назначение и описание контактов основного разъема

Номер контакта	Название	Назначение, цвет подсоединяемого провода
1	COM2	Реле сирены, общий контакт, оранжевый
2	SEN	Датчик двери, белый
3	NO2	Реле сирены, нормально-разомкнутый контакт, зеленый
4	BUT	Кнопка «Выход», серый
5	NC1	Реле замка, нормально-замкнутый контакт, желтый
6	GND	GND, черный
7	COM1	Реле замка, общий контакт, красный
9	NO1	Реле замка, нормально-разомкнутый контакт, синий

Таблица 4. Назначение и описание контактов разъема Wiegand

Номер контакта	Название	Назначение, цвет подсоединяемого провода
1	WD1-OUT	Wiegand – данные «1», белый
2	WD0-OUT	Wiegand – данные «0», зеленый

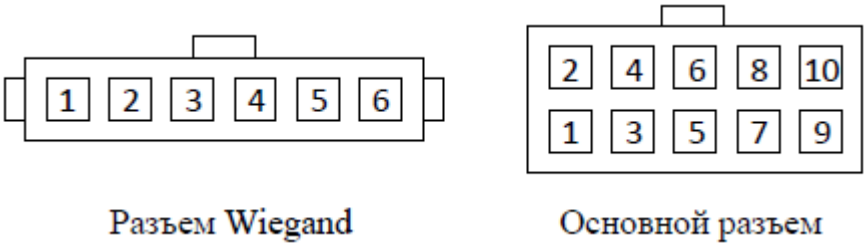


Рисунок 3. Нумерация контактов разъемов контроллера

Подключение и отключение проводов следует проводить только при отключённом питании контроллера.
В первую очередь следует подсоединить провод выравнивания потенциалов (GND), что позволит предотвратить электростатическое повреждение контроллера.

Провод электропитания следует подсоединить к контроллеру в последнюю очередь.

Неправильное подсоединение проводов к контроллеру может привести к выходу из строя считывателя отпечатков пальцев или электронных компонентов контроллера.

3.3 Подключение к контроллеру периферийного оборудования

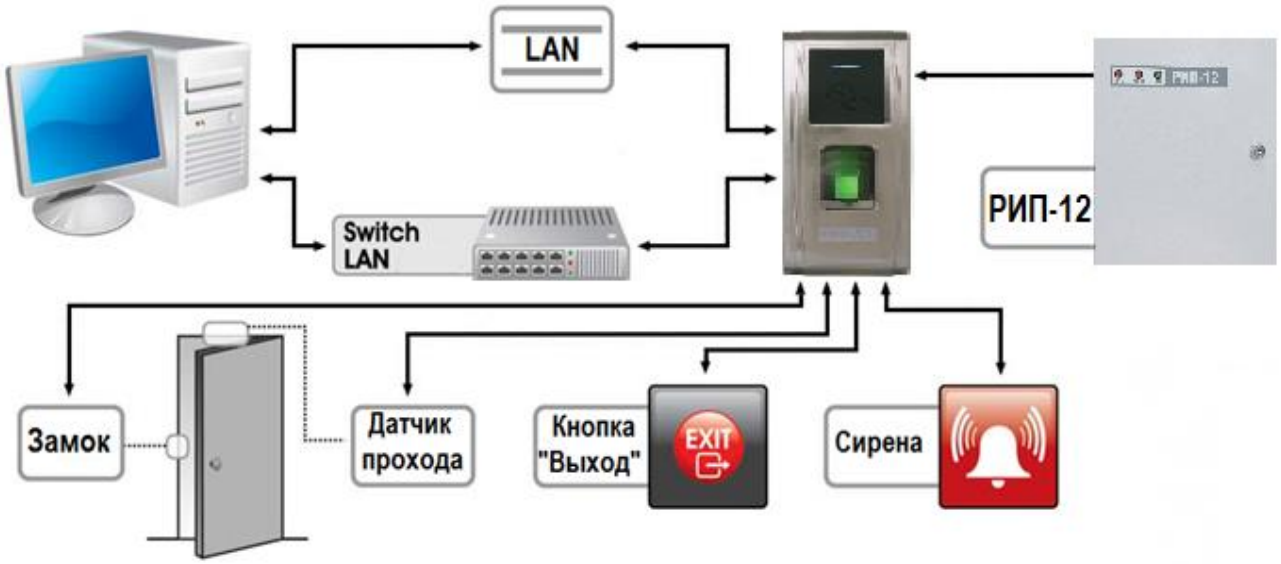
К контроллеру можно подсоединить:

- датчик двери, который используется для определения положения двери (открыта/закрыта). Контроллер может выявлять несанкционированный проход через дверь и включать сигнал тревоги, если дверь была открыта неавторизованным пользователем (взломана) или удержана в открытом положении слишком долго.

- звуковые оповещатели с напряжением питания 12 В.

- кнопку выход.

- электрический замок (электромагнитный (защёлка) или электромеханический).



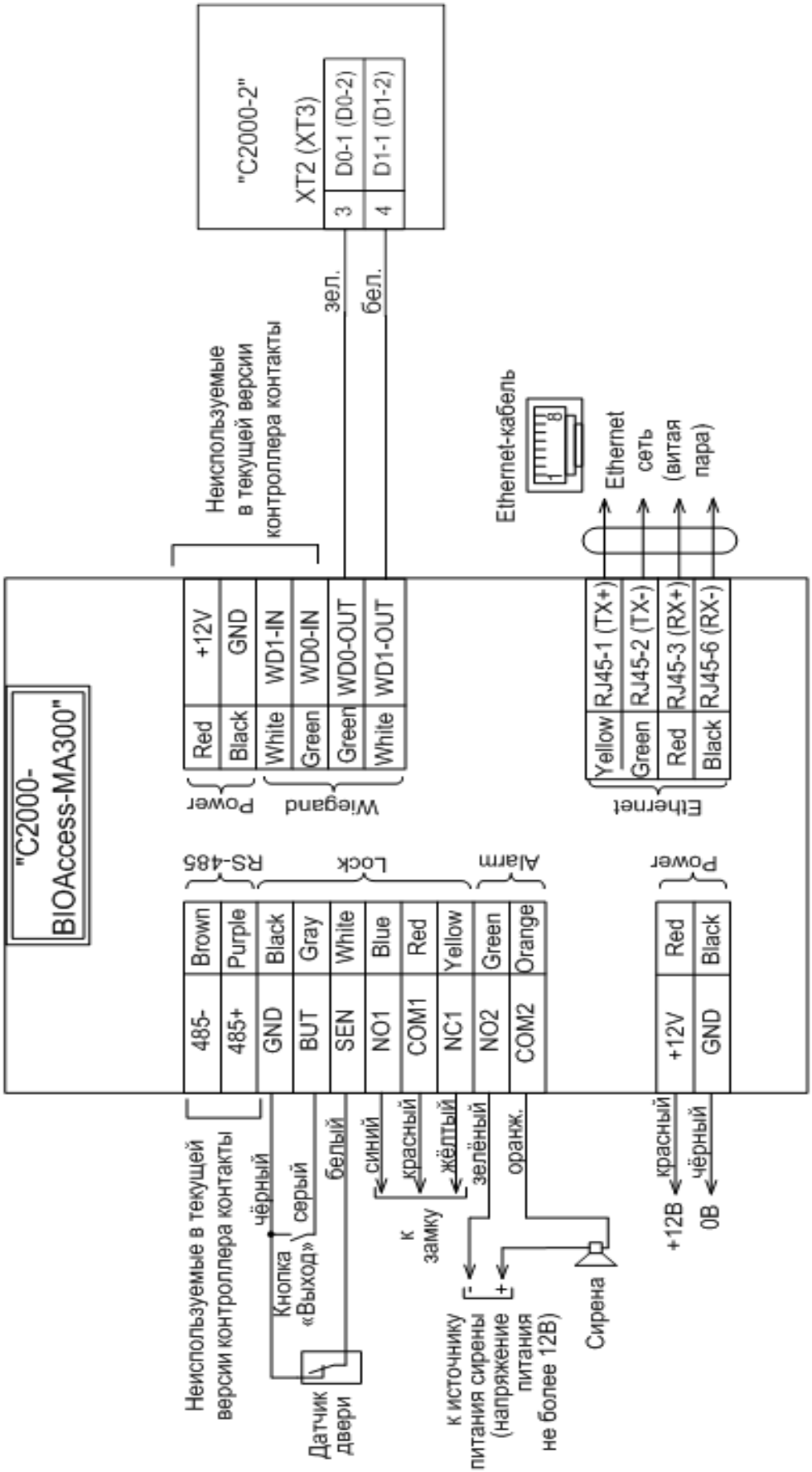


Рисунок 4. Схема подключений к контроллеру

Электромагнитный замок (защелка) может питаться от того же источника питания, что и контроллер, либо от отдельного источника питания. При питании от одного источника цепи питания контроллера и питания замка должны быть выполнены различными парами проводов, которые объединяются только на клеммах источника питания. Кроме того, необходимо параллельно обмотке замка установить диод в обратном включении (допустимый ток диода в прямом направлении должен быть не менее 1 А), диод входит в комплект поставки. На рис. 5 приведены рекомендуемые схемы подключения замков.

Рисунок 5. Рекомендуемые схемы подключения замков (разъём J10)

3.4 Подключение к ПК

Для связи контроллеров с компьютером используется сеть Ethernet.

На рис. 6, 7 приведены схемы подключения контроллеров по интерфейсу Ethernet.

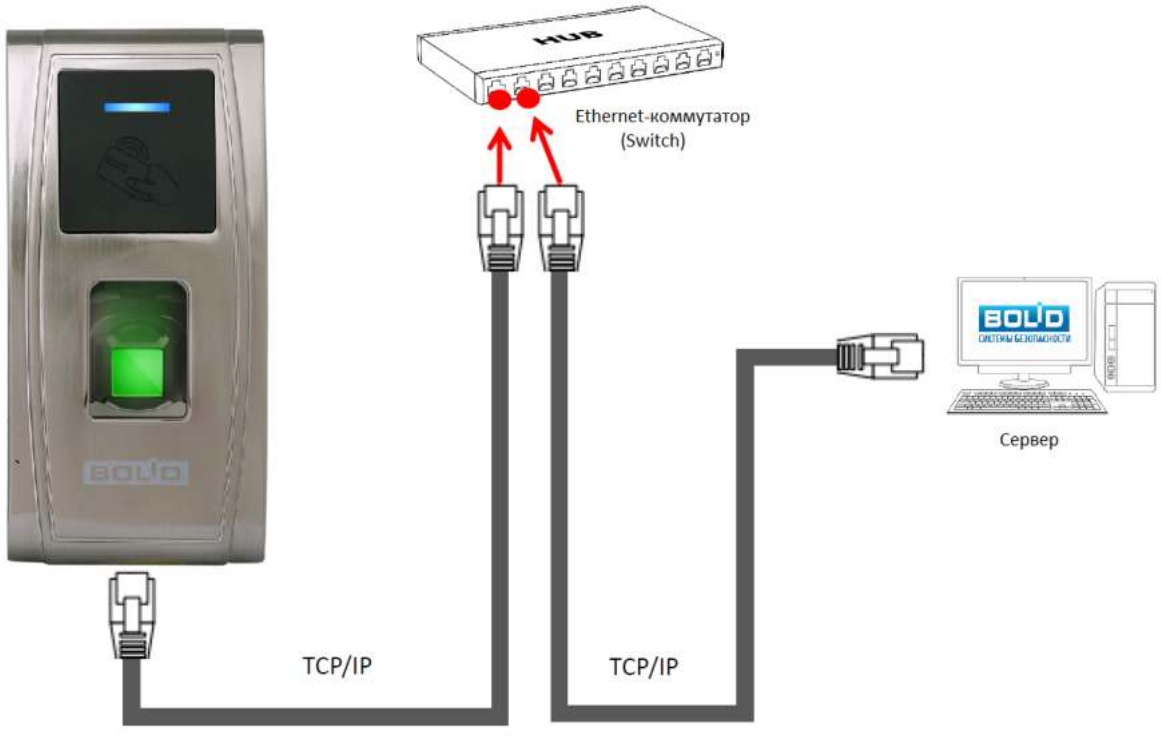


Рисунок 6. Подключение контроллера к ПК через Ethernet-коммутатор (Switch)

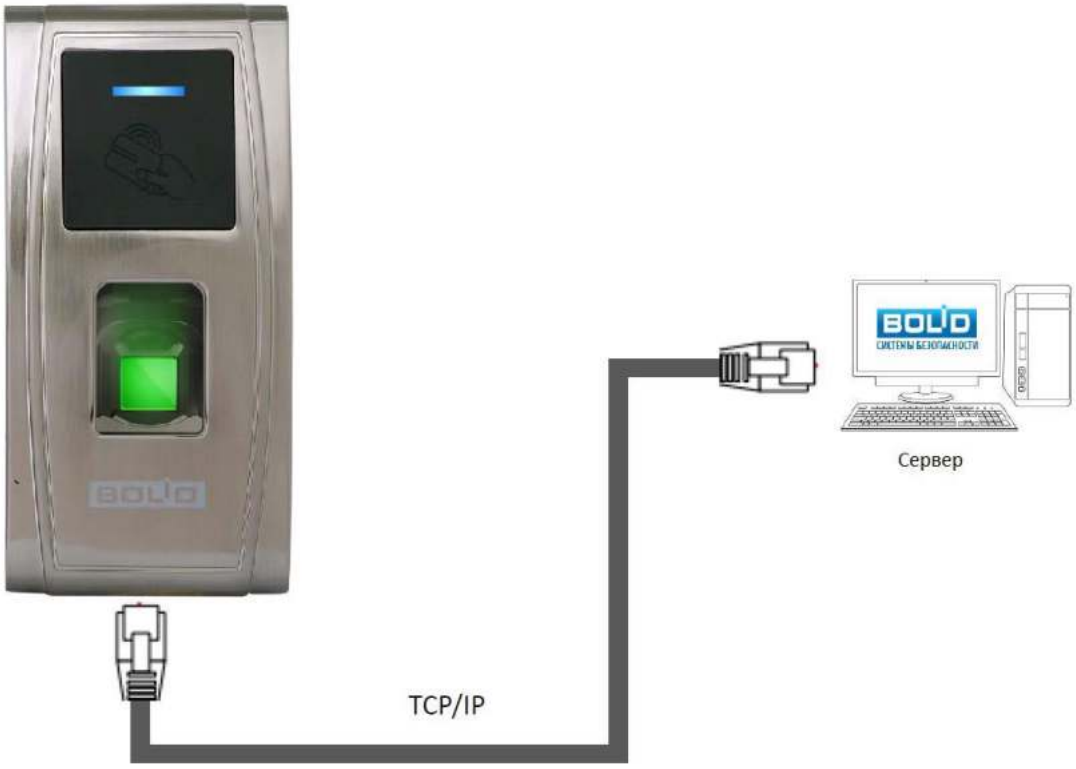


Рисунок 7. Подключение контроллера к ПК напрямую

При подключении контроллера к ПК напрямую используется crossover-кабель.

4 Базовая настройка контроллера

4.1 Автономная работа

При использовании контроллера в автономном режиме (без АРМ «Орион Про»), его следует подключить к ПК и провести настройку при помощи программы BAProg.

После настройки рекомендуется создать резервную копию шаблонов отпечатков пальцев на жёстком диске ПК или на другом накопителе информации.

4.1.1 Настройка контроллера в BAProg

Стандартная последовательность настройки контроллера перед началом эксплуатации в программе BAProg следующая:

1. Программирование окон времени.
2. Настройка групп доступа.
3. Регистрация пользователей.
4. Редактирование времени управления замком.

Запустите программу BAProg. Во вкладке «Конфигурация» в разделе «Подключение нового контроллера» укажите параметры подключаемого прибора – «IP-адрес» и «Порт». После этого нажмите на кнопку «Подключить новый прибор». Программа попытается подключить контроллер с указанными параметрами. Если подключение произошло успешно, то слева в списке подключённых приборов появится новый контроллер.

BAProg запоминает информацию обо всех подключаемых контроллерах, поэтому при очередном запуске для подключения к конкретному прибору достаточно выполнить двойной щелчок левой кнопкой мыши по названию контроллера в списке «Приборы».

Начиная с версии Ver 6.60 Jul 20 2016 в контроллере предусмотрена процедура сброса сетевых настроек.
Для предыдущих версий сброс возможен только в сервисном центре ЗАО НВП «Болид». При этом вся информация будет удалена из памяти контроллера.

В поле «Замок» следует задать время управления замком. Установленное в контроллере время управления замком можно увидеть при нажатии на кнопку «Считать». Новое значение, указываемое в строке «Время управления замком, сек», можно записать с помощью кнопки «Записать».

Так же следует задать следующие параметры:

– **Пауза до вкл. сирены, с** – время (от 1 до 99), через которое включается сигнал тревоги при блокировке открытой двери. Если установлено значение параметра «0», то сигнал тревоги не включается;

– **Контакты двери** – данный параметр может иметь следующие значения:

- «Откр» – для нормально разомкнутых датчиков двери;
- «Закр» – для нормально замкнутых датчиков двери;
- «Нет» – если датчик двери не используется.

– **Вкл. сирену после, попыток** – в случае нескольких попыток неудачной аутентификации подряд может быть включён сигнал тревоги. Количество попыток (от 1 до 9). Если установлено значение параметра «0», то сигнал тревоги не включается.

Сброс сетевых настроек осуществляется с помощью магнитного «тампера». Магнит расположен на кронштейне. Для удобства сброса рекомендуется снять кронштейн и отсоединить от него магнит. Для сброса сетевых настроек контроллера следует выполнить следующие шаги:

1. При выключенном питании поднести магнит к «тамперу» и удерживать его («тампер» расположен в выемке в задней крышке контроллера).
2. Включить питание, дождаться загрузки контроллера.
3. Убрать магнит и подождать 30 секунд.
4. Три раза поднести магнит к «тамперу», после каждого поднесения контроллер выдаст один звуковой сигнал.

После сброса сетевые настройки будут следующими:
IP-адрес: 192.168.1.201
Маска: 255.255.255.0
Порт: 4370
Если сброс не удался, то следует повторить процедуру.

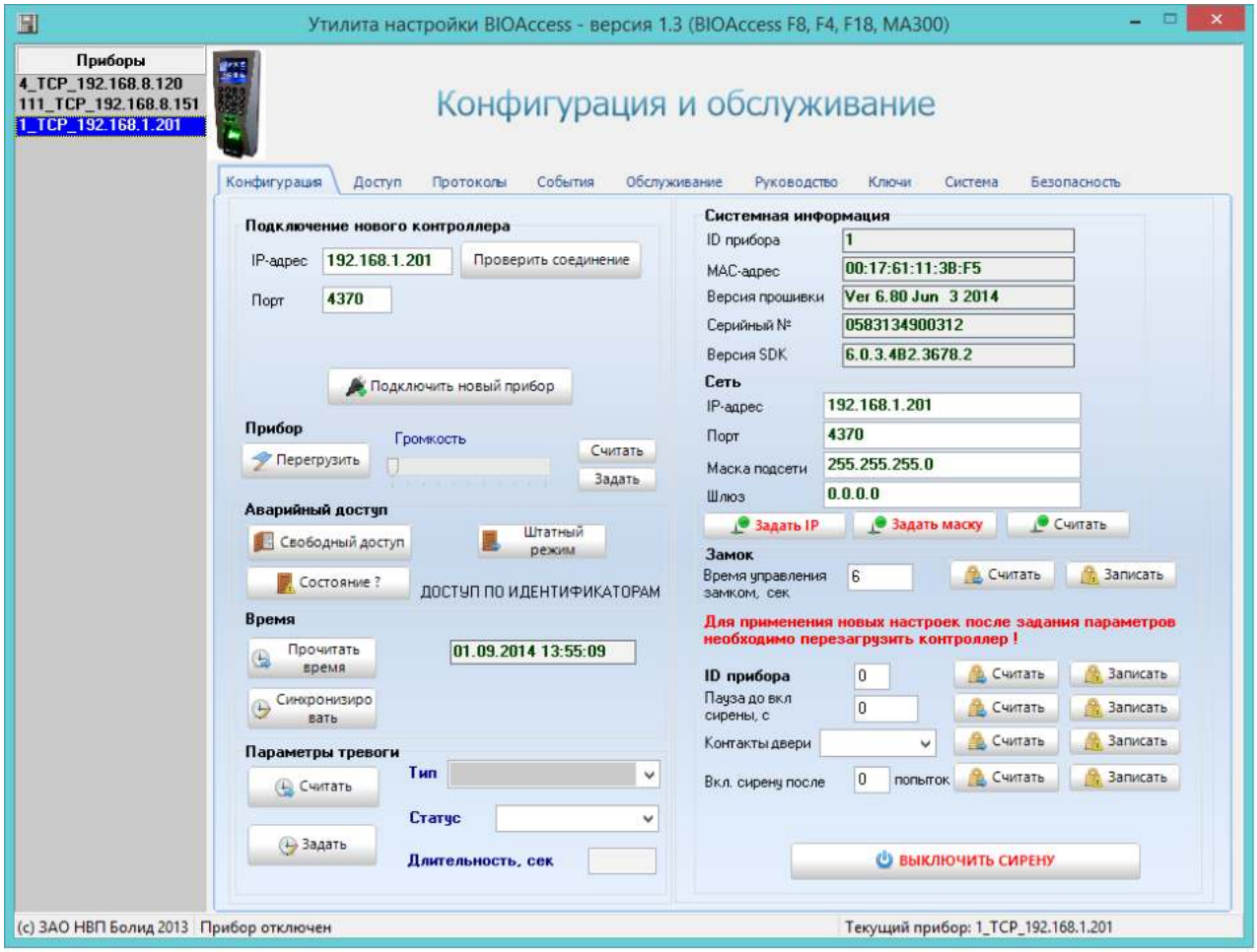


Рисунок 8. Окно «Конфигурация и обслуживание»

После подключения прибора к программе BAProg следует провести его начальную настройку, для этого перейдите во вкладку «Обслуживание»

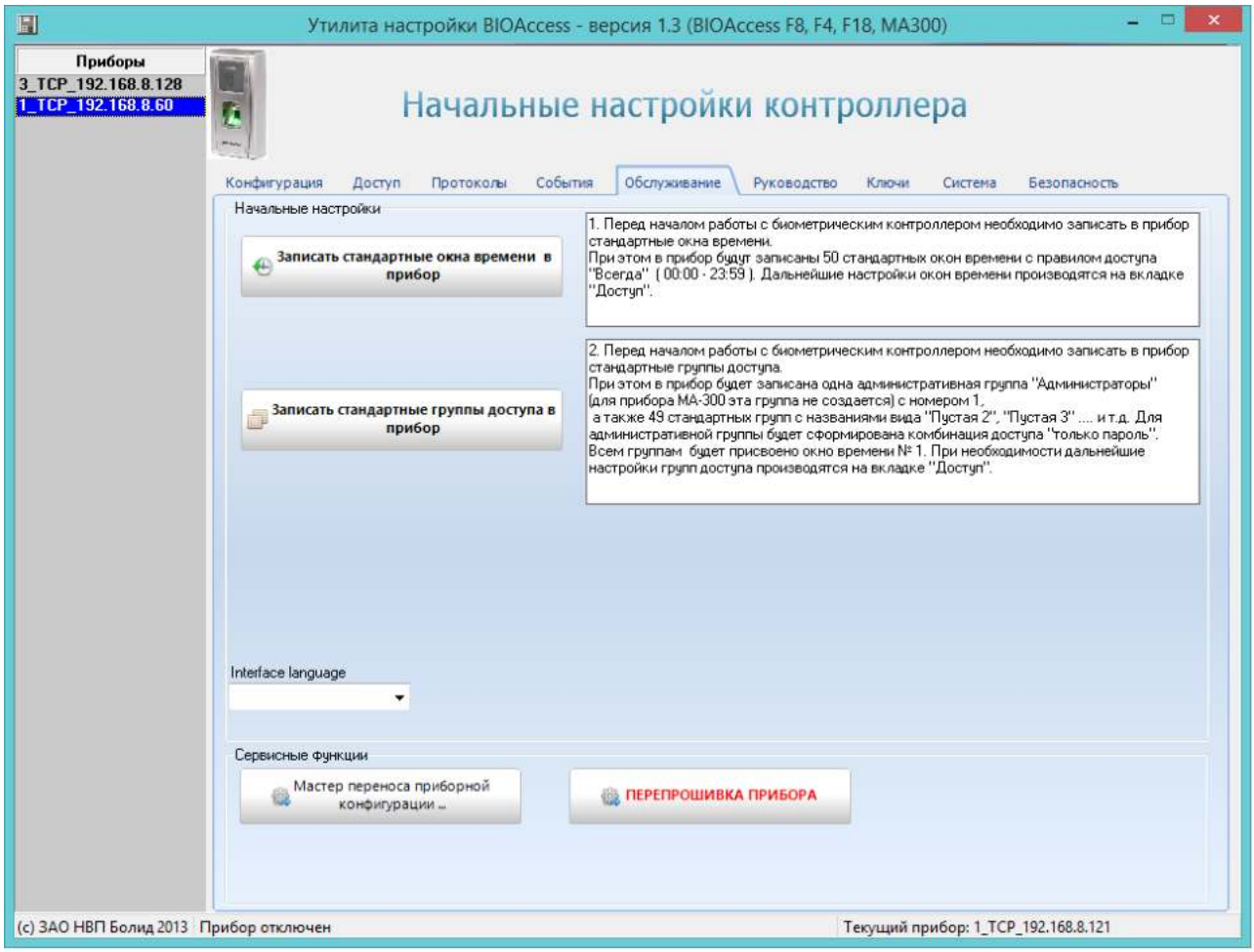
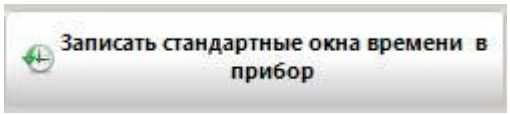
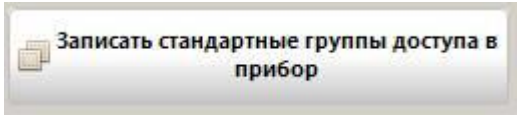


Рисунок 9. Окно «Начальные настройки контроллера»

После этого последовательно нажмите кнопки, подтверждая запросы программы:





4.1.2 Добавление пользователей и временных окон

Для добавления пользователей и временных окон перейдите во вкладку «Доступ». В левой части вкладки расположен список зарегистрированных пользователей, в котором отображается номер (ID) и имя пользователя (Имя). В центральной части показана основная информация о выделенном сотруднике.

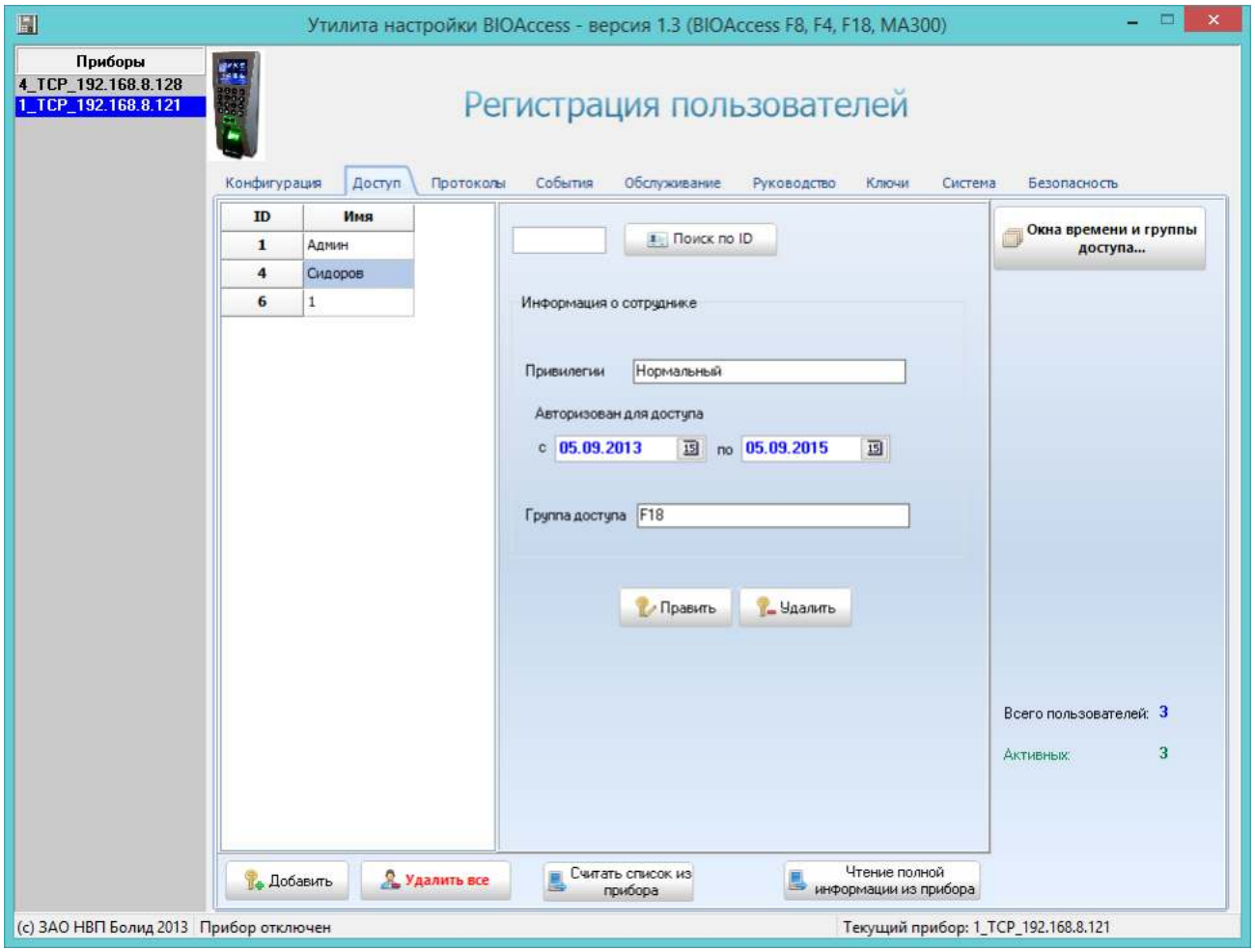
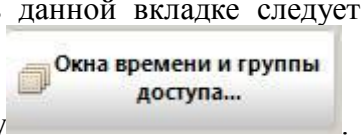


Рисунок 10. Окно «Регистрация пользователей»

Первоначально, в данной вкладке следует настроить группы и окна времени, для этого нажмите кнопку 

. После этого откроется окно настройки групп доступа и окон времени:

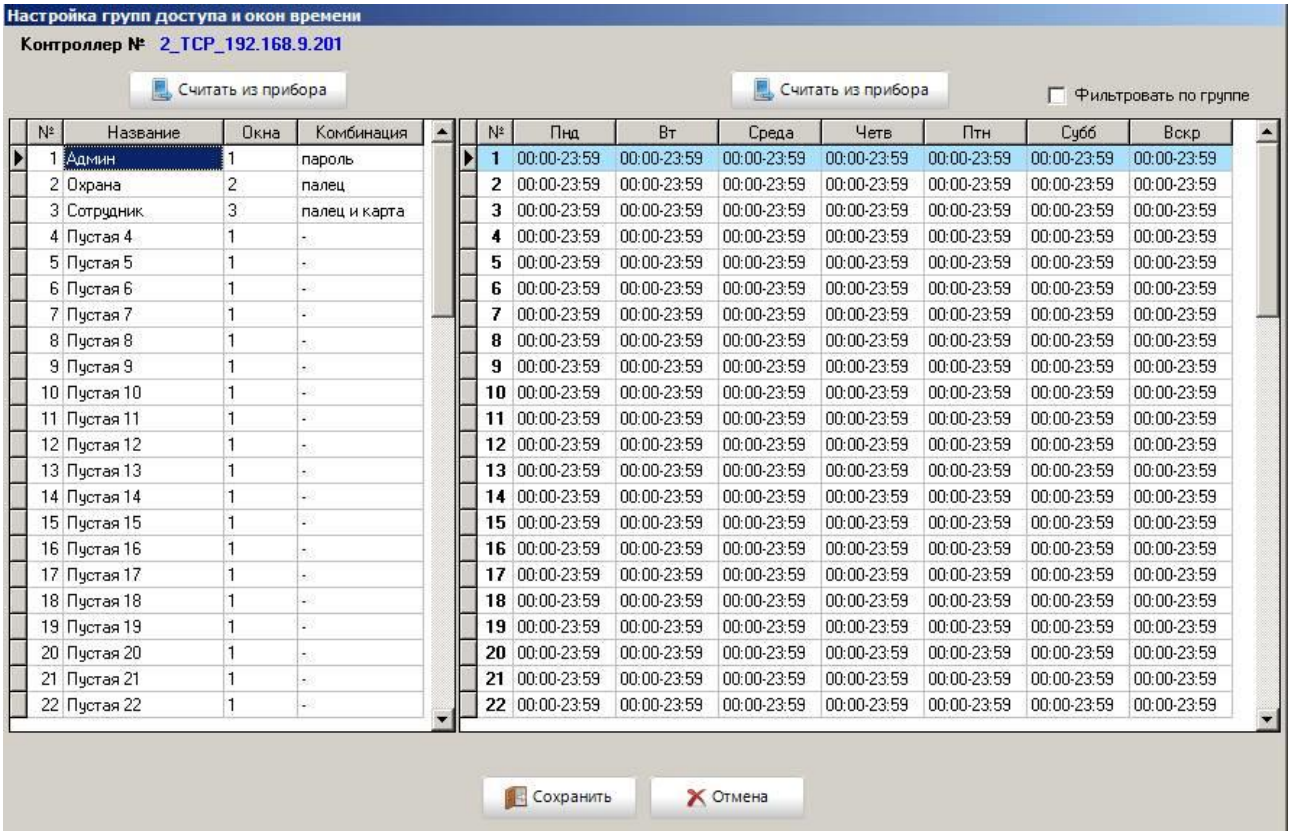


Рисунок 11. Окно «Настройка групп доступа и окон времени»

В правой части окна настройки групп доступа и окон времени необходимо провести настройку окон времени, следует выполнить двойной щелчок левой кнопкой мыши по необходимой строке, откроется окно «Редактирование окна времени»:

Рисунок 12. Окно «Редактирование окна времени»

В левой части окна настройки групп доступа и окон времени следует выполнить двойной щелчок левой кнопкой мыши по необходимой строке, откроется окно ввода данных:

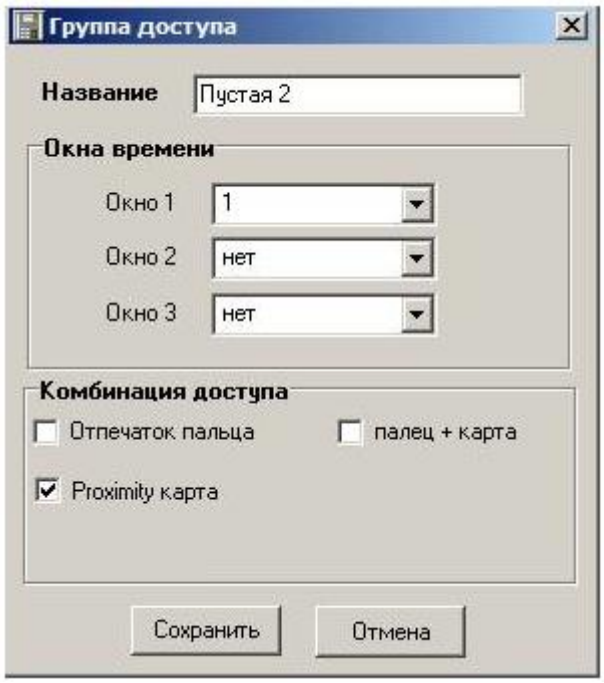


Рисунок 13. Окно «Группа доступа»

Для добавления нового пользователя следует нажать кнопку Добавить, откроется окно ввода данных.

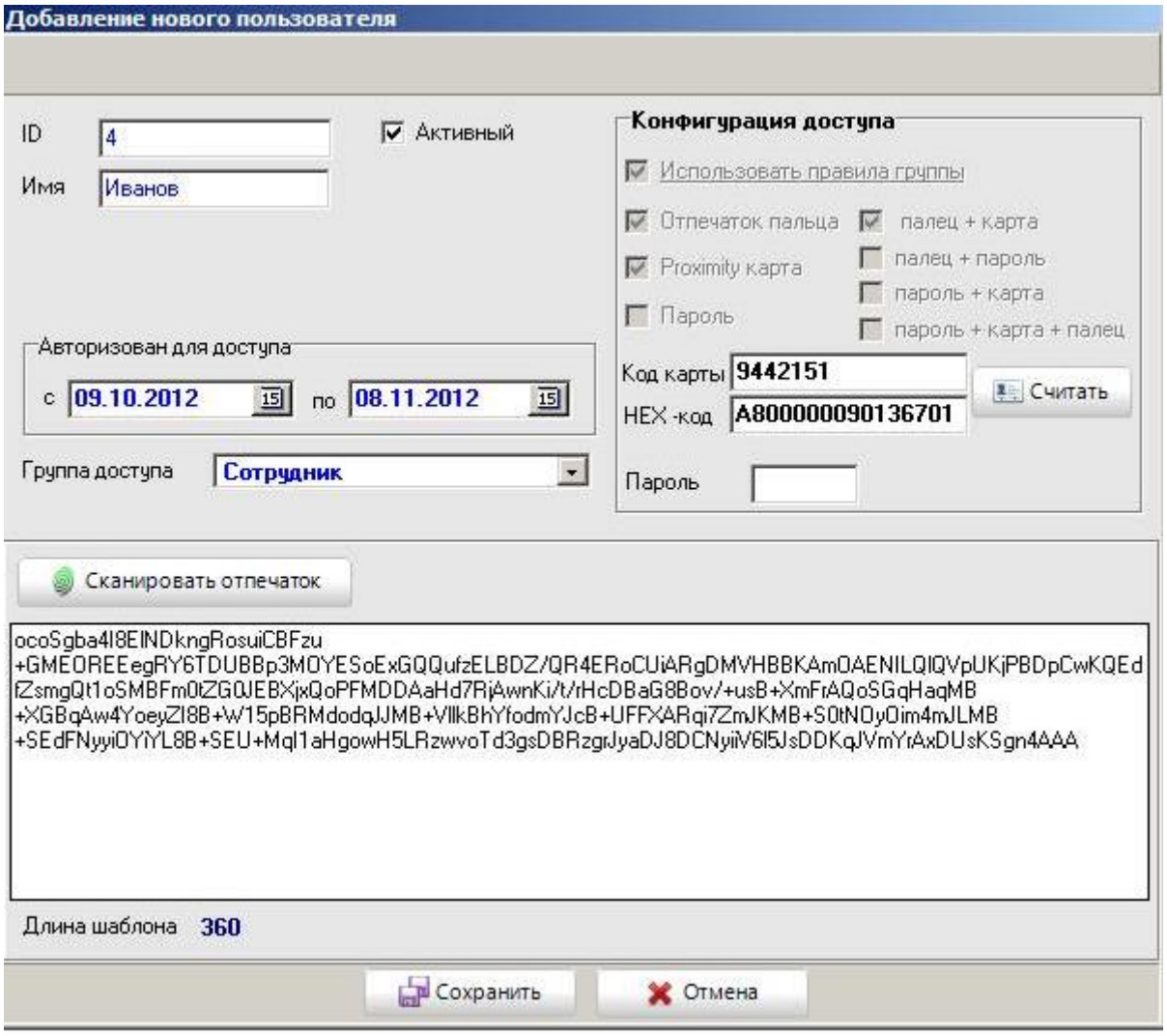


Рисунок 14. Окно «Добавление нового пользователя»

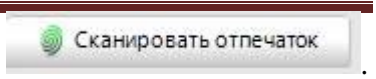
Следует указать порядковый номер пользователя в общем списке пользователей (ID) и имя пользователя (Имя).

В поле «Авторизован для доступа» следует указать интервал времени, в течение которого для пользователя сохраняется статус «Активный», позволяющий пользователю совершать проход через дверь согласно правам доступа.

Следует выбрать необходимую группу доступа, заданную ранее.

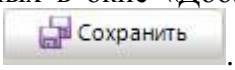
В зависимости от настроек группы становится возможным зарегистрировать код Proximity-карты и/или отпечаток пальца.

1) Для считывания кода карты следует поднести карту к контроллеру и после этого нажать на кнопку Считать. В полях «Код карты» и «HEX-код» появятся считанные значения.

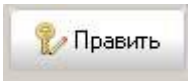
2) Для сканирования отпечатка пальца следует нажать на кнопку 

. При этом появляется сообщение:

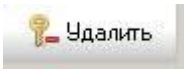
Для сканирования отпечатка следует приложить нужный палец к сканеру три раза подряд. Если сканирование завершилось успешно, то в поле сканирования отпечатка пальца появится шаблон отпечатка пальца. Если отсканировать отпечаток не удалось, то поле останется пустым.

После ввода всех необходимых данных в окне «Добавление нового пользователя» для их сохранения следует нажать на кнопку 

.

При помощи кнопки 

производится редактирование данных уже введенных пользователей.

При помощи кнопки 

производится удаление введенных пользователей.

4.2 Работа контроллера в составе АРМ «Орион Про»

Настройку работы контроллера в составе ИСО «Орион-Про» следует проводить в соответствии с Руководством по эксплуатации АРМ «Орион Про» (пункт 6.2.7).

5 Обслуживание

Рекомендуемая частота очистки:

Оптическая поверхность сканера – не рекомендуется частая чистка. Допускается работа сканера при появлении жирной плёнки и видимых загрязнений. Очистка рекомендуется только при заметном ухудшении качества считывания.

6 Гарантии изготовителя (поставщика)

Гарантийный срок эксплуатации – 18 месяцев со дня ввода изделия в эксплуатацию, но не более 24 месяцев со дня выпуска изготовителем.

При направлении изделия в ремонт к нему обязательно должен быть приложен акт с описанием возможной неисправности и **указанием сетевых настроек контроллера (IP-адрес, маска подсети, шлюз).**

Рекламации направлять по адресу:

ЗАО НВП «Болид», 141070, Московская область, г. Королёв, ул. Пионерская, д. 4.

Тел./факс: (495) 775-71-55 (многоканальный), 777-40-20, 516-93-72.

E-mail: info@bolid.ru. http://bolid.ru

7 Сведения о сертификации

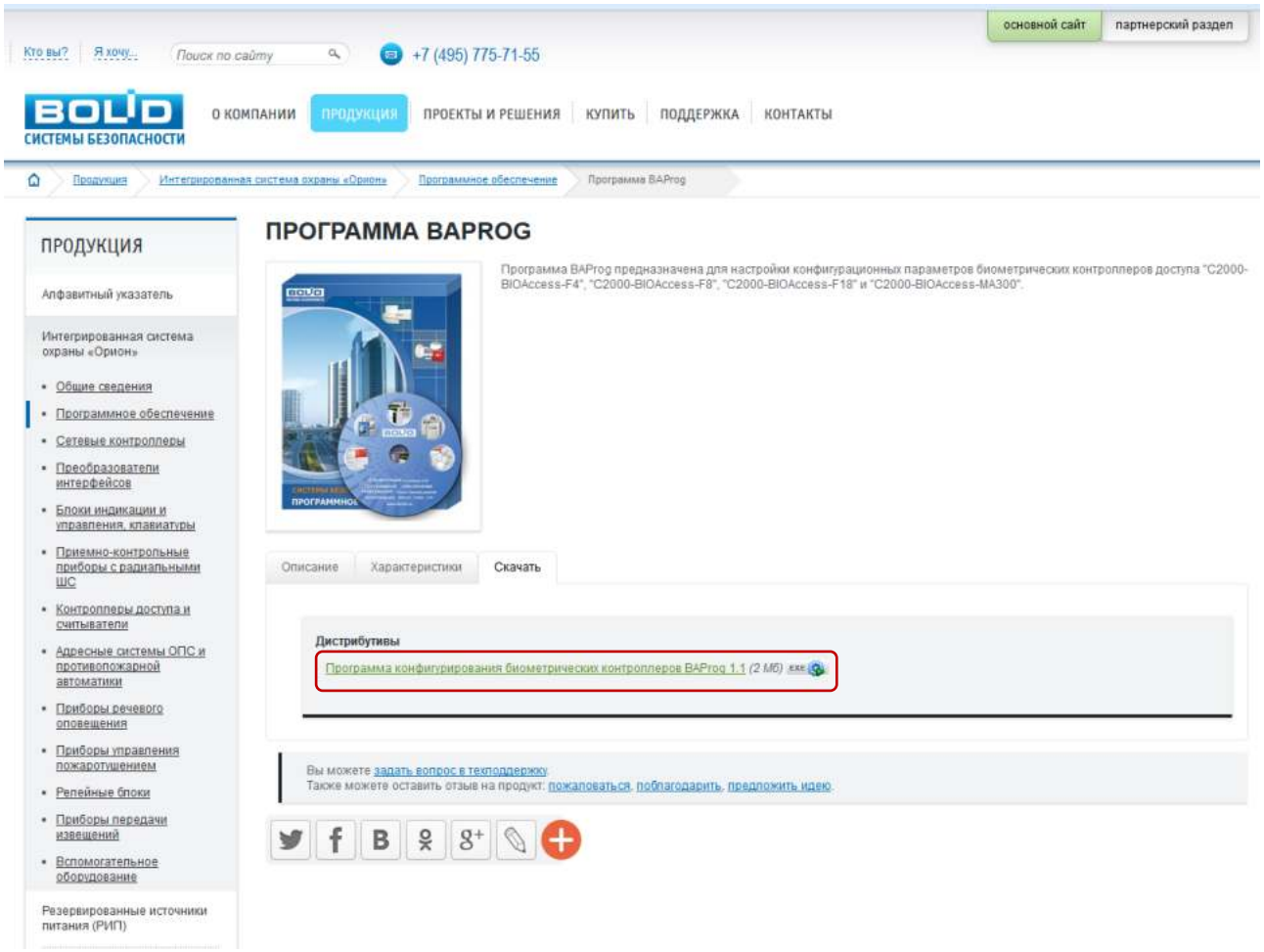
7.1 Биометрический контроллер доступа «С2000-BIOAccess-MA300» соответствует требованиям технического регламента Таможенного союза ТР ТС 020/2011. Имеет сертификат соответствия № RU C-RU.ME61.B.01316.

7.2 Биометрический контроллер доступа «С2000-BIOAccess-MA300» имеет сертификат соответствия технических средств обеспечения транспортной безопасности требованиям к их функциональным свойствам № МВД РФ.03.000037.

Приложение 1

Установка программы BAProg

Новейшую версию программы BAProg можно скачать с сайта http://bolid.ru/production/orion/po-orion/baprog.html.



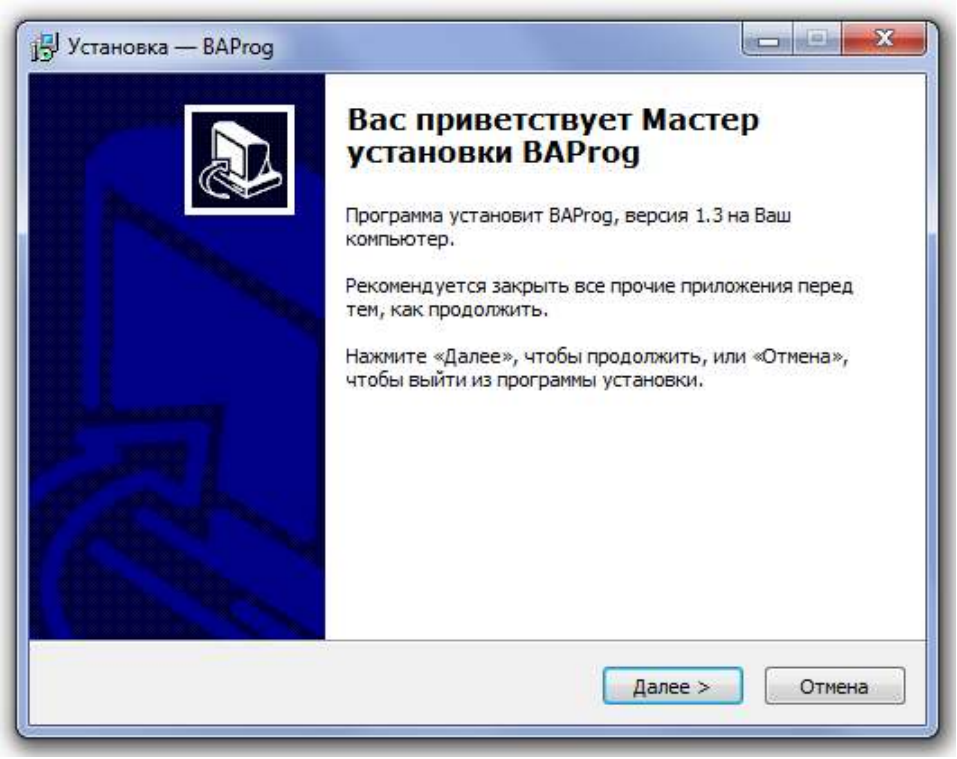
Минимальные системные требования BAProg:

- Процессор: 300 МГц
- Оперативная память: 128 МБ
- Видеоадаптер и монитор: SVGA (800×600)
- Свободное место на HDD: 6 МБ
- Аппаратный порт: RJ-45, USB
- Другое: клавиатура, мышь
- Операционная система: Windows XP, Windows Vista, Windows 7, Windows 8.

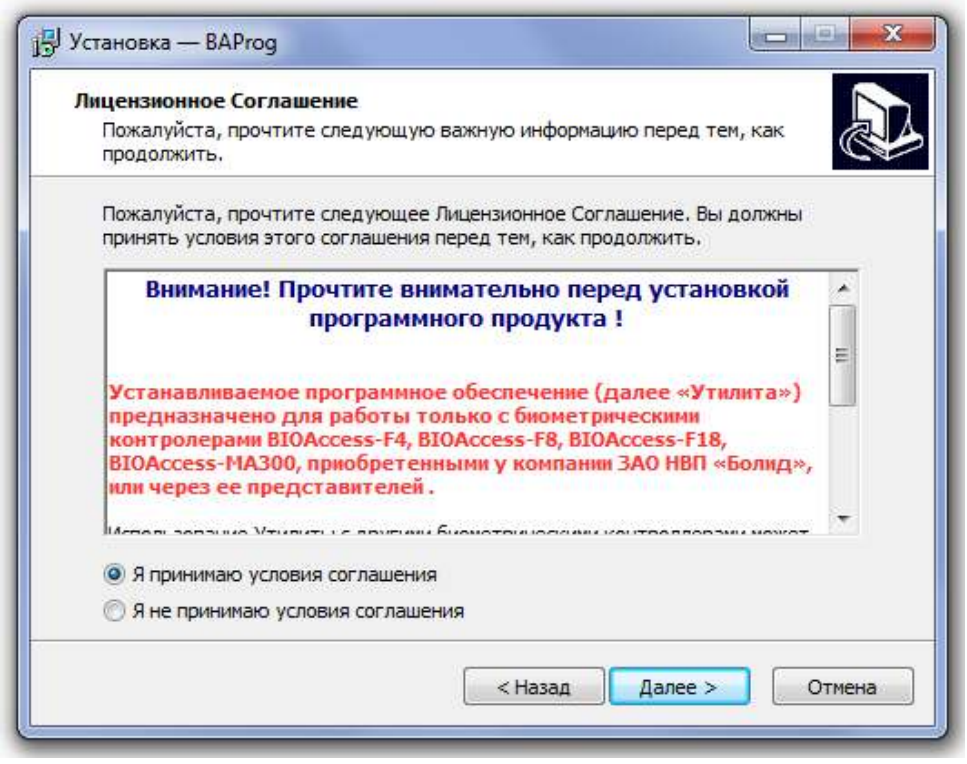
BAProg предоставляется в виде установочного файла с расширением *.exe*.

В операционных системах Windows Vista, 7, 8 запуск установочного файла должен производиться от имени администратора.

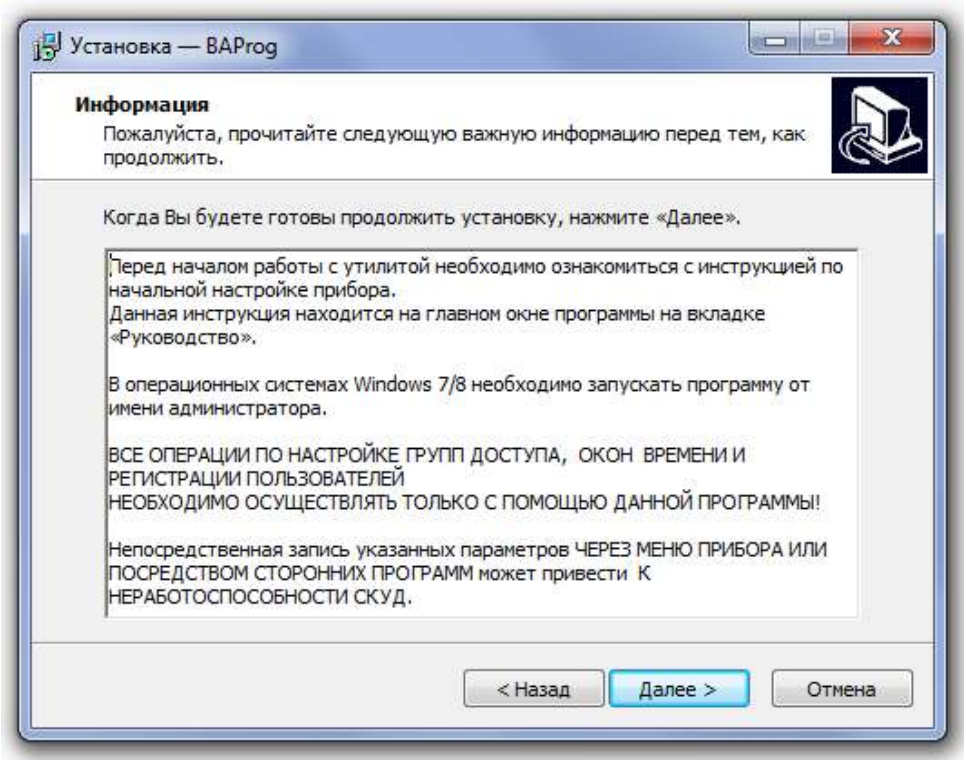
При запуске программы установки появляется следующее окно:



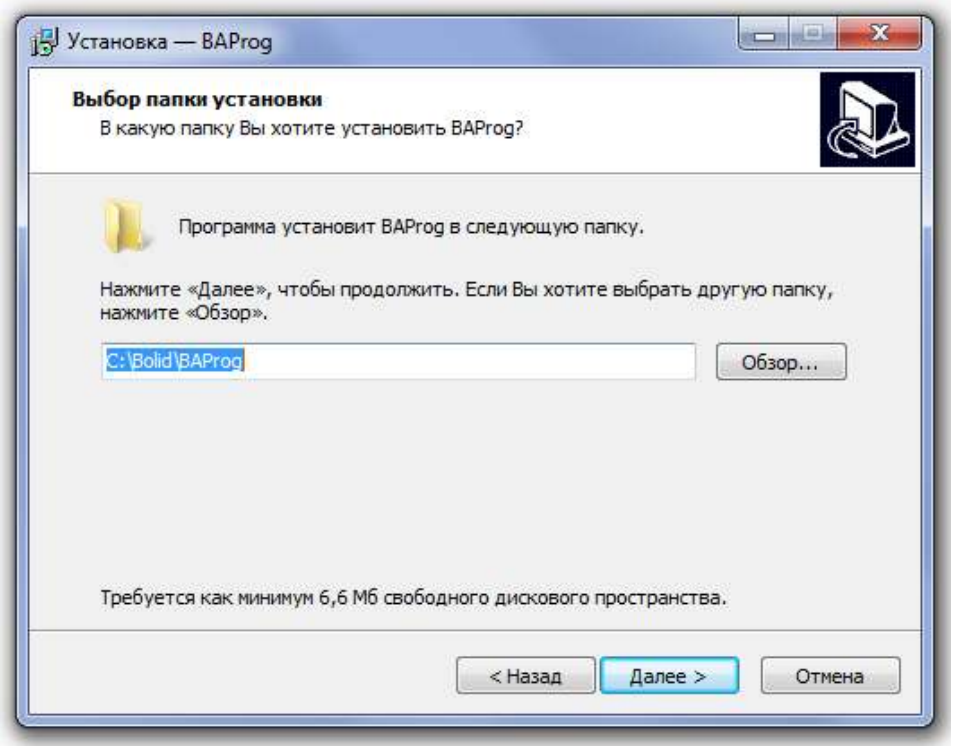
Нажмите на кнопку «Далее >». В появившемся окне, после прочтения соглашения, отметьте пункт «Я принимаю условия соглашения» и нажмите кнопку «Далее >».



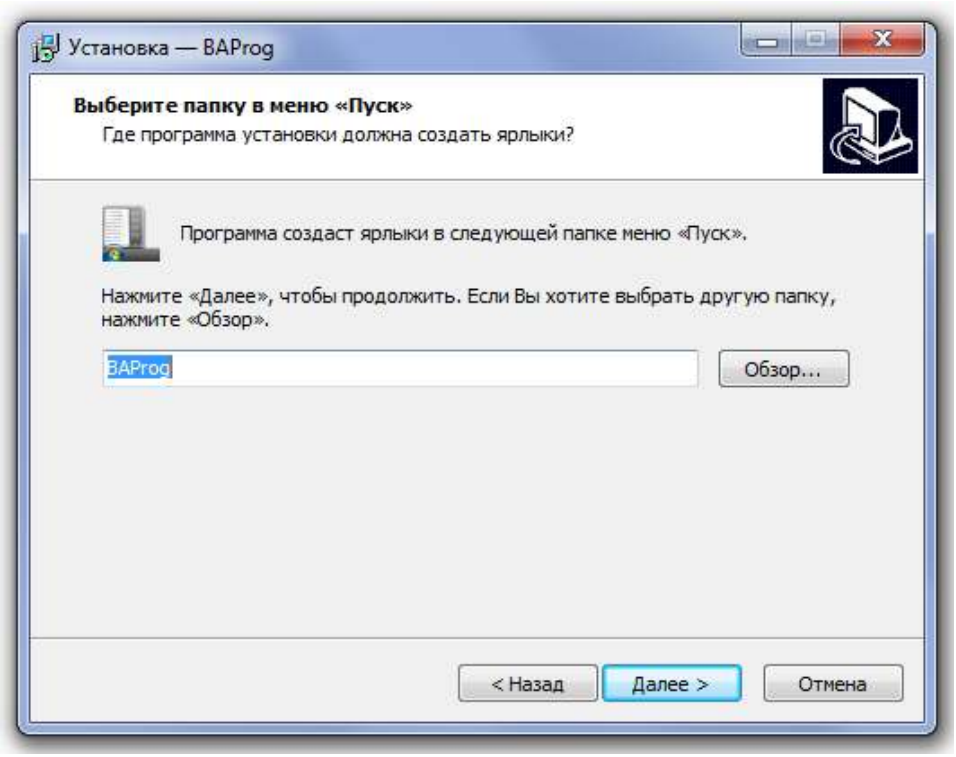
Прочитав информацию в появившемся окне, нажмите кнопку «Далее >».



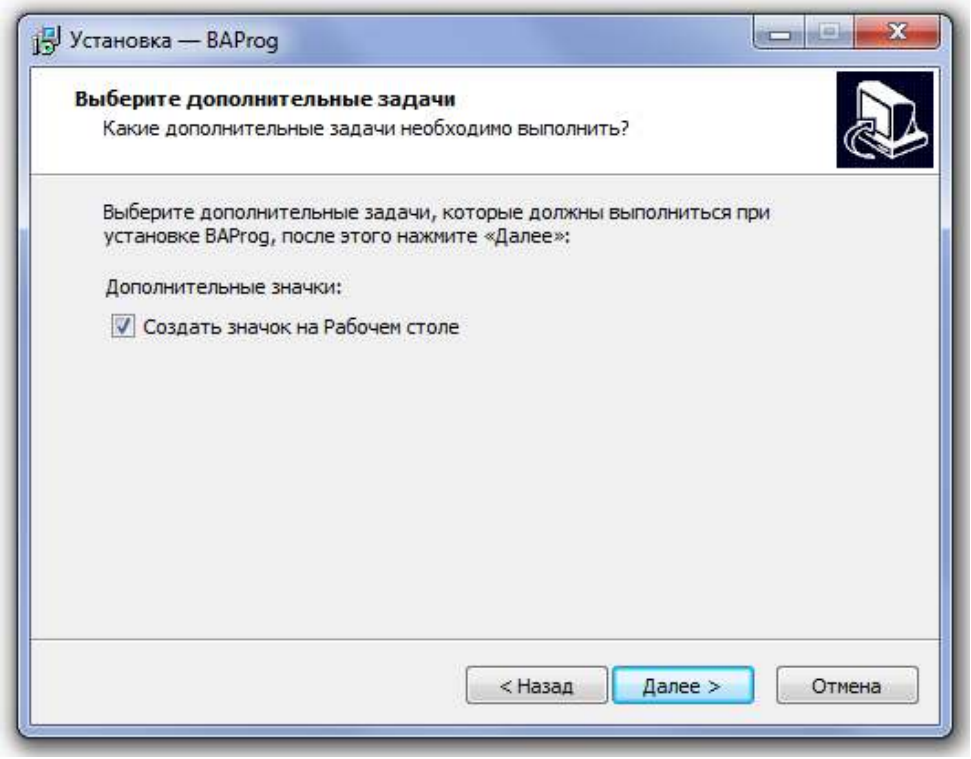
В следующем окне укажите путь для установки программы и нажмите на кнопку «Далее >».



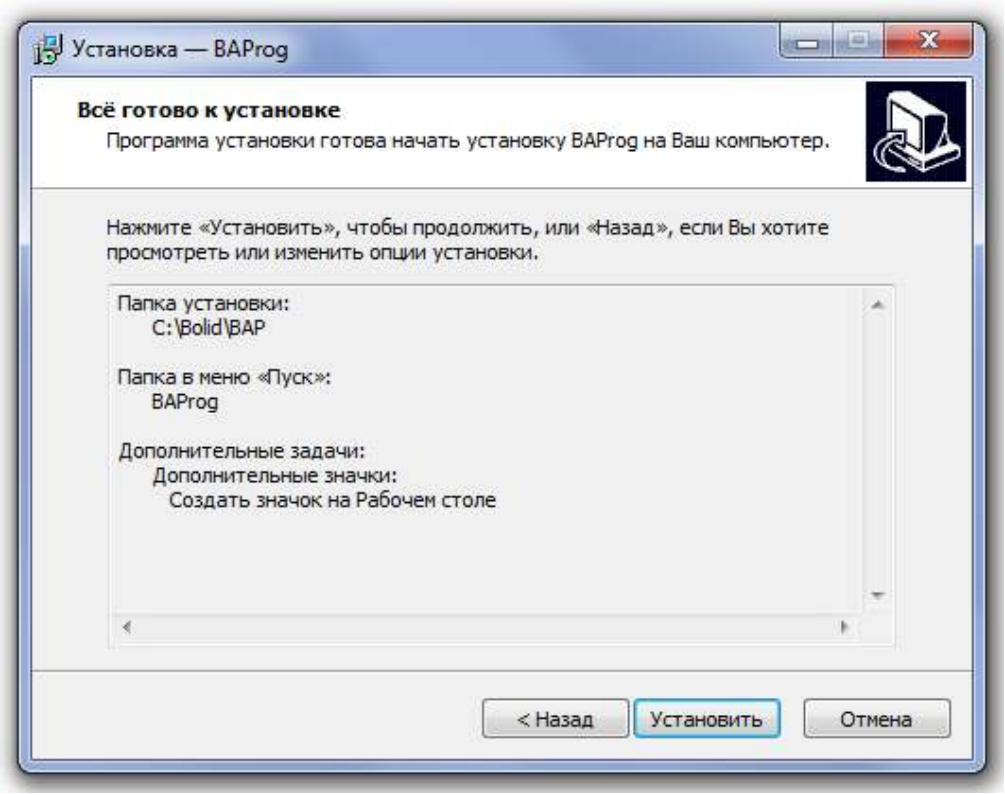
В следующем окне укажите название папки в меню «Пуск», в которой будут размещены ярлыки программы BAProg, и нажмите на кнопку «Далее >».



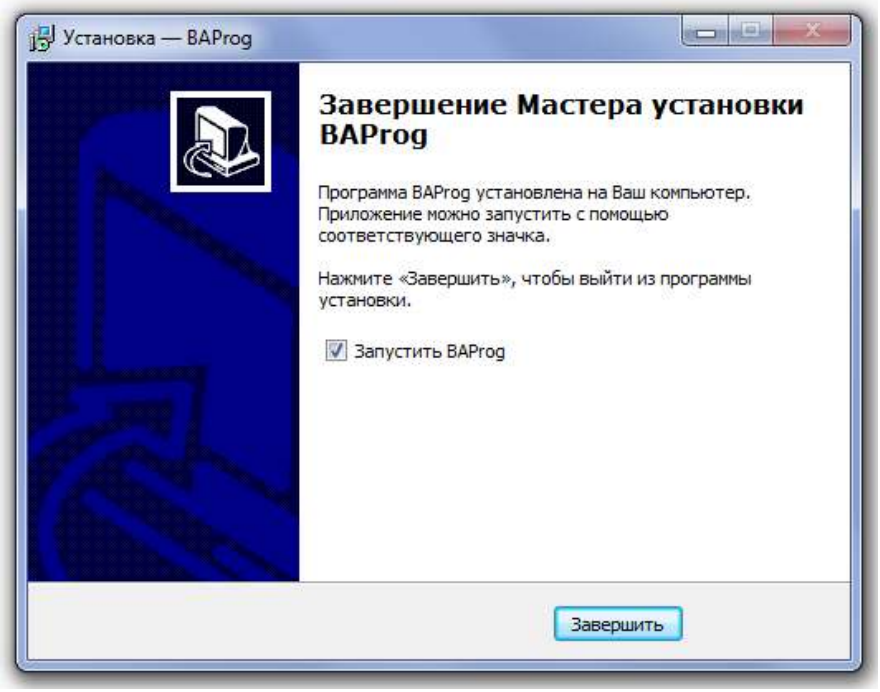
В следующем окне при необходимости включите опцию «Создать значок на Рабочем Столе». Нажмите на кнопку «Далее >».



В следующем окне проверьте пути установки программы и нажмите на кнопку «Установить».



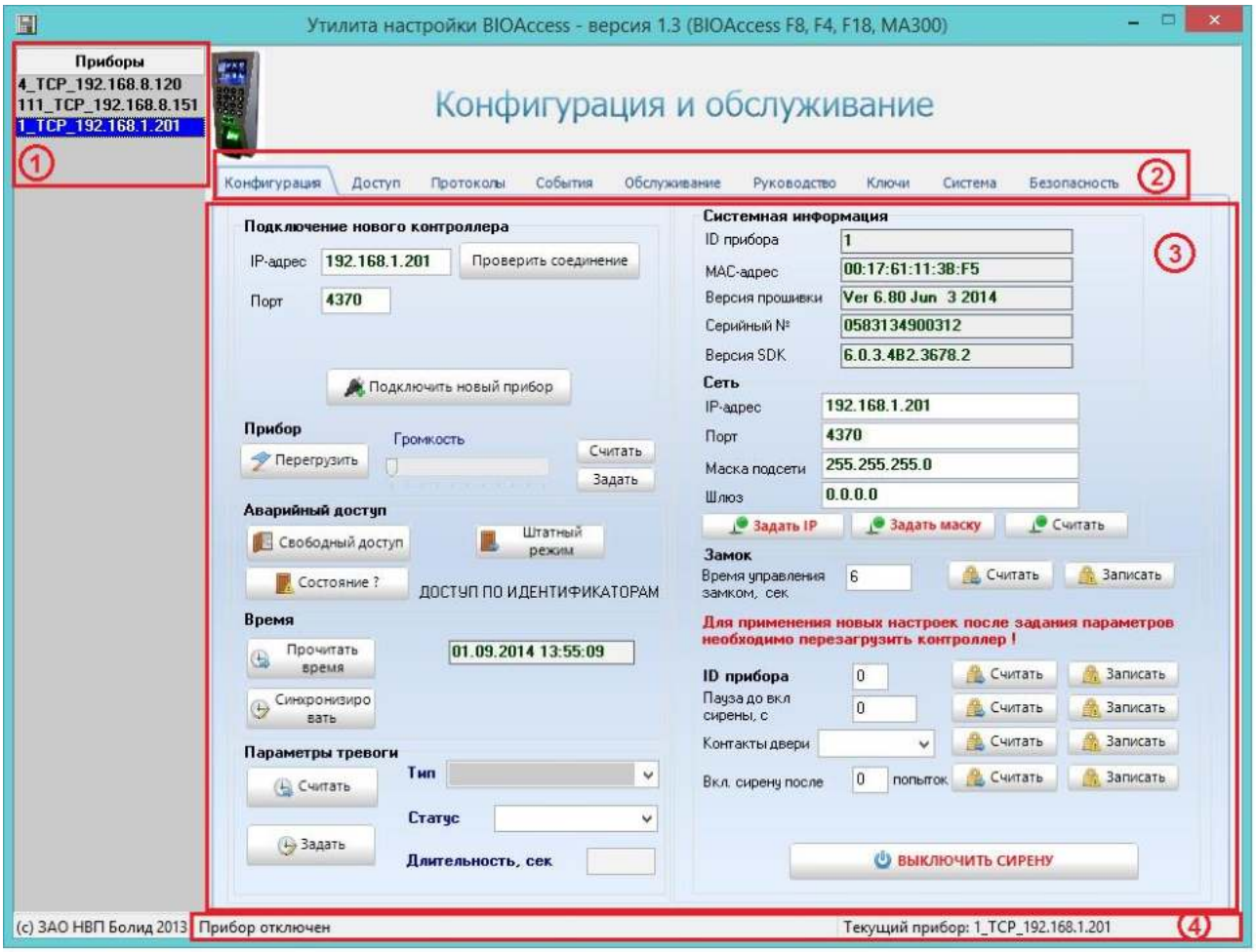
После установки программы появляется следующее окно, в котором по умолчанию включена опция «Запустить BAProg». Если не отключать эту опцию и нажать на кнопку «Завершить», то будет запущена программа BAProg.



Приложение 2

Описание интерфейса программы BAProg

При запуске окно BAProg выглядит следующим образом:



Элементы окна BAProg:

1. Список подключённых приборов.
2. Список вкладок.
3. Рабочая область вкладки.
4. Строка статуса.

В BAProg рабочие инструменты распределены по следующим вкладкам:

- Конфигурация
- Доступ
- Протоколы приборов
- События
- Обслуживание
- Руководство

- Ключи
- Система
- Безопасность

Далее рассмотрим инструменты, расположенные на каждой из этих вкладок.

Вкладка «Конфигурация»

На этой вкладке расположены следующие группы элементов:

- Подключение нового контроллера
- Прибор
- Аварийный доступ
- Время
- Системная информация
- Сеть
- Замок

В разделе «Подключение нового контроллера» указываются параметры подключаемых приборов – «IP-адрес» и «Порт». Если необходимо проверить, доступен ли контроллер по сети Ethernet, то для проверки физического соединения можно использовать кнопку «Проверить соединение». Если соединение присутствует, то после нажатия под кнопкой отобразится текст «Ping OK», в противном случае – «Ping НЕТ ОТВЕТА». Наличие физического соединения, как правило, гарантирует работоспособность и доступность самого контроллера, однако не всегда гарантирует корректную работу.

Кнопка «Перегрузить» в поле «Прибор» позволяет перезагрузить операционную систему контроллера.

В поле «Аварийный доступ» расположены кнопки управления реле двери:

- Предоставить – открыть дверь. Включается режим свободного доступа, без предъявления идентификаторов.
- Штатный режим – восстановить штатный режим. Включается режим доступа по идентификаторам.
- Состояние ? – справа от кнопки показывается текущий режим доступа.

В поле «Время» можно посмотреть системное время контроллера (кнопка «Прочитать время») и синхронизировать системное время контроллера с системным временем ПК (кнопка «Синхронизировать»).

Кнопки «Считать», расположенные в полях «Системная информация» и «Сеть» позволяют увидеть значения соответствующих параметров контроллера.

Кнопки «Задать IP» и «Задать маску» позволяют задать IP-адрес и сетевую маску контроллера. При использовании этих кнопок необходимо учитывать, что за один раз можно сменить только один параметр – адрес или маску. При этом после каждого такого изменения, необходимо удалить и вновь добавить контроллер в список приборов. При проведении данных операций есть риск «потерять» сетевое соединение с контроллером после смены его адреса или сетевой маски. Поэтому рекомендуется пользоваться этими возможностями при прямом соединении кабелем Ethernet рабочего компьютера и контроллера, что позволяет при необходимости оперативно «подстроить» параметры сетевой

карты компьютера (IP-адреса и сетевой маски) для возможности восстановления соединения с прибором.

В поле «Замок» можно редактировать время управления замком. Установленное в контроллере время управления замком можно увидеть при нажатии на кнопку «Считать». Новое значение, указываемое в строке «Время управления замком, сек», можно записать с помощью кнопки «Записать».

В разделе «Параметры тревоги» можно задать параметры управления различными видами тревог (Взлом корпуса прибора, Ошибка идентификации, Взлом двери). В выпадающем списке «Тип» можно выбрать нужный вид тревоги, а в полях «Статус» и «Длительность» задать режим ее работы, то есть Запрещена/Разрешена данная тревога, и время звучания сирены по данной тревоге в секундах.

На вкладке так же можно задать следующие параметры:

– ID прибора – номер прибора;

– Пауза до вкл. сирены, с – время (от 1 до 99), через которое включается сигнал тревоги при блокировке открытой двери. Если установлено значение параметра «0», то сигнал тревоги не включается;

– Контакты двери – данный параметр может иметь следующие значения:

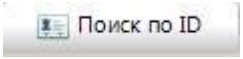
- «Откр» – для нормально разомкнутых датчиков двери;
- «Закр» – для нормально замкнутых датчиков двери;
- «Нет» – если датчик двери не используется.

– Вкл. сирену после, попыток - в случае нескольких попыток неудачной аутентификации подряд (например, несколько раз подряд введён неверный пароль) может быть включён сигнал тревоги. Количество попыток (от 1 до 9). Если установлено значение параметра «0», то сигнал тревоги не включается.

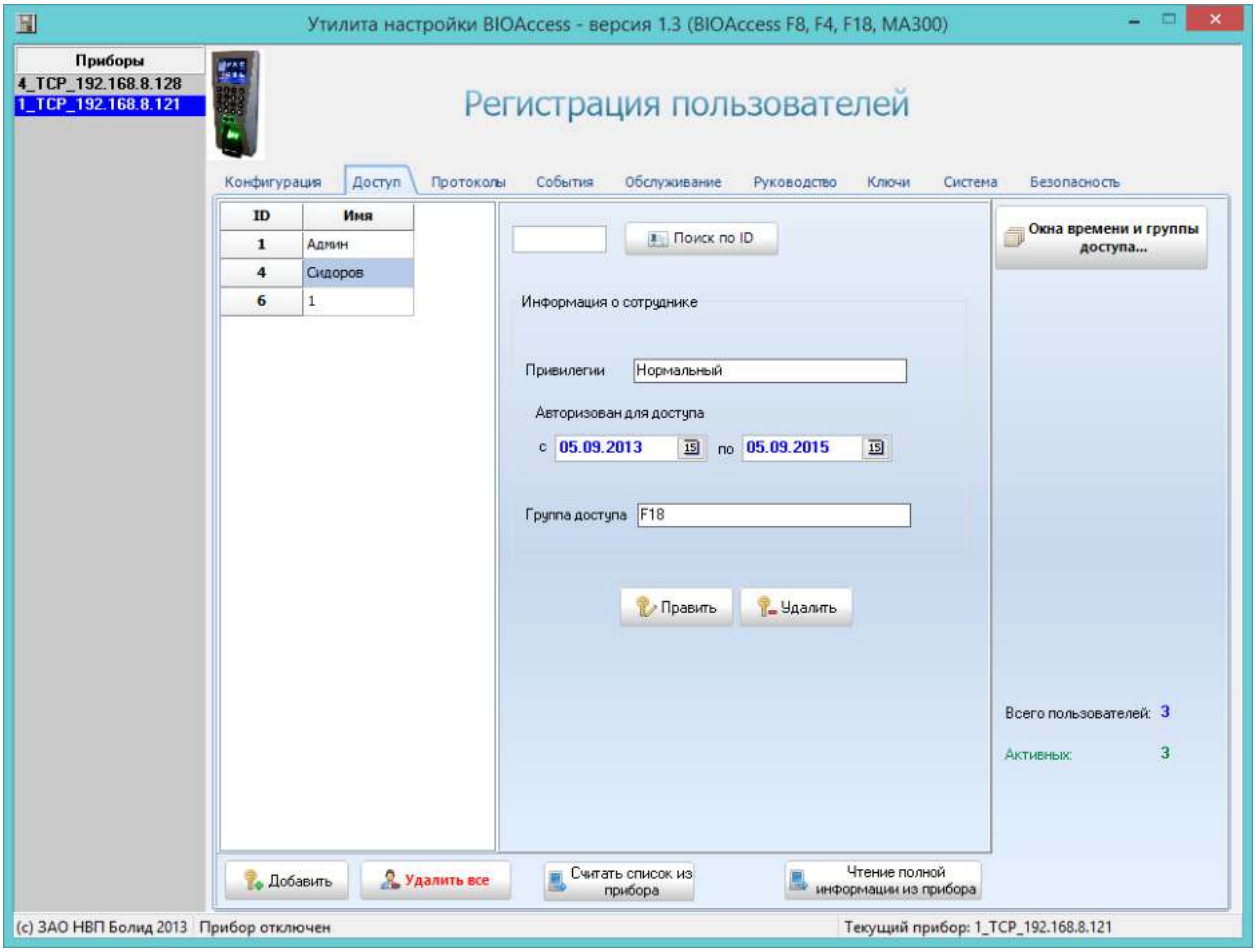
Вкладка «Доступ»

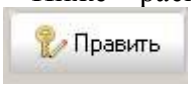
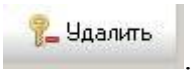
На вкладке «Доступ» осуществляется управление правами доступа зарегистрированных пользователей. В левой части вкладки расположен список зарегистрированных пользователей, в котором указывается номер (ID) и имя пользователя (Имя).

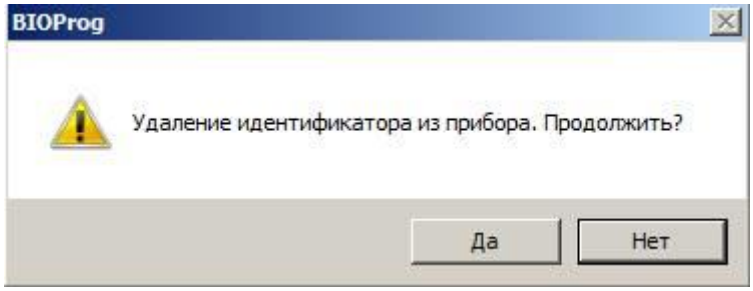
В средней части вкладки можно осуществить поиск пользователя по номеру пользователя.

Для этого нужно указать нужный номер в поле слева от кнопки 

и нажать на кнопку.



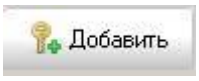
Также в средней части вкладки «Доступ» показывается основная информация для выбранного пользователя. Ниже расположены кнопки редактирования информации о выбранном пользователе:  и  . При нажатии на кнопку «Править» появляется окно «Редактирование информации о пользователе», аналогичное окну «Добавление нового пользователя» (рис. 21). При нажатии на кнопку «Удалить» появляется запрос на подтверждение операции:

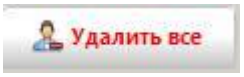


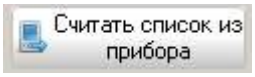
Для удаления информации о пользователе нужно нажать на кнопку «Да».

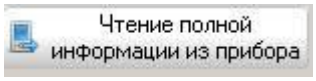
Также на вкладке «Доступ» показывается общее количество пользователей («Всего пользователей») и количество активных пользователей («Активных»).

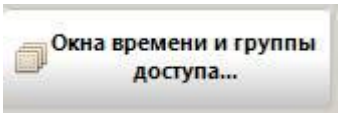
На этой же вкладке расположены кнопки:

- 

– добавление нового пользователя;
- 

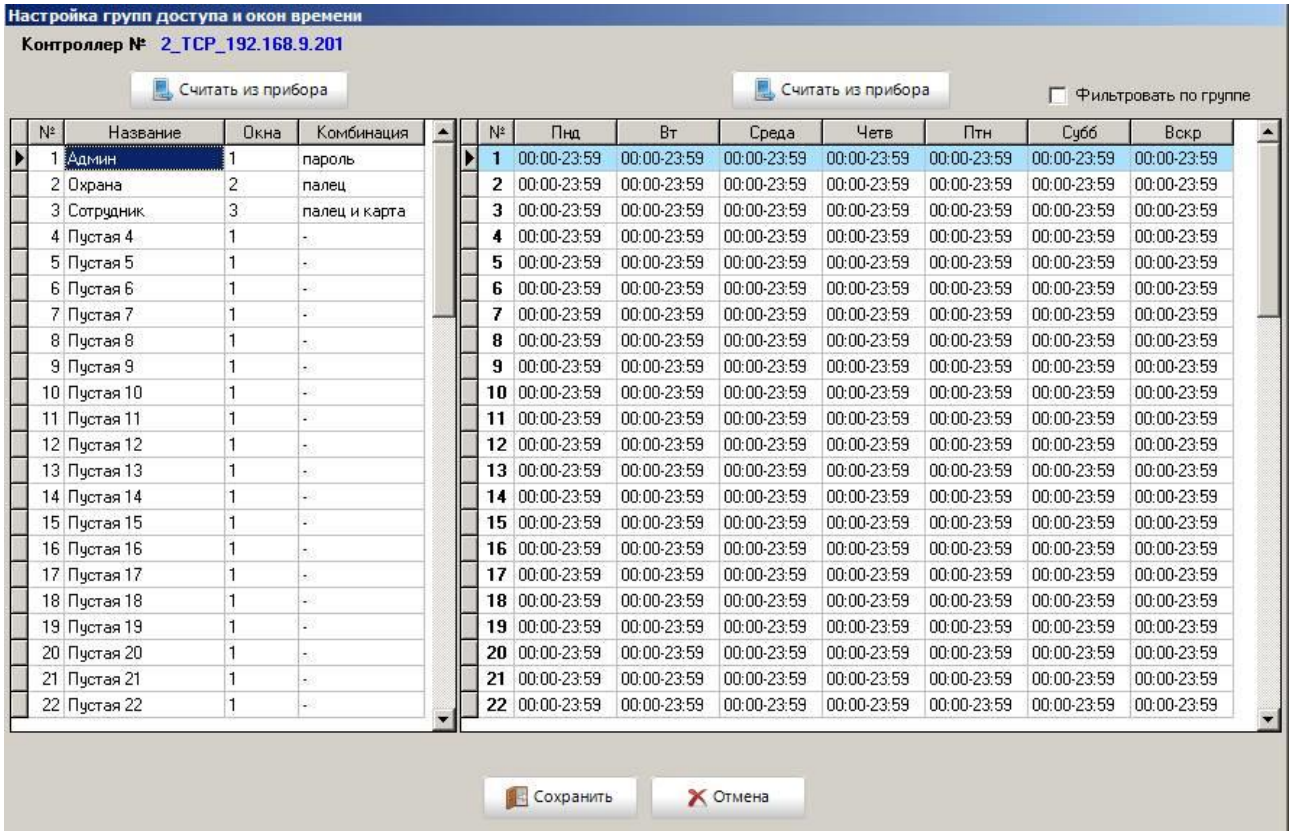
– удаление всех пользователей;
- 

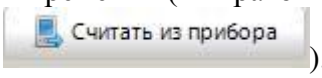
– чтение списка пользователей из контроллера;
- 

– чтение из контроллера списка пользователей и информации о пользователях;
- 

– редактирование окон времени и групп доступа.

При нажатии на кнопку «Окна времени и группы доступа...» появляется следующее окно:



В окне «Настройка групп доступа и окон времени» показаны список групп доступа (в левой части) и список окон времени (в правой части). Каждый список можно прочитать из контроллера (кнопка 

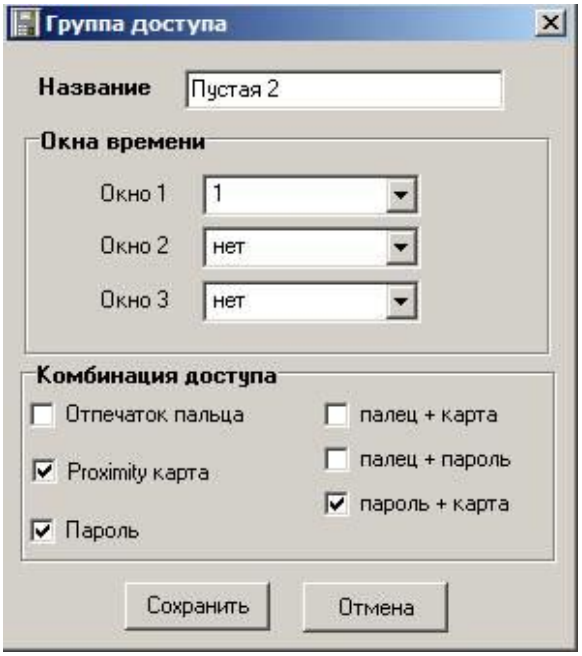
).

Если включить опцию «Фильтровать по группе», то при выборе в левой части окна группы доступа в правой части окна показываются только окна времени, назначенные выбранной группе доступа.

Для редактирования выбранного окна времени нужно выполнить двойной щелчок левой кнопкой мыши на соответствующей строке в списке окон времени. При этом появляется окно «Редактирование окна времени»:

В этом окне можно указать нужные интервалы времени для каждого дня недели. Кнопка «Полный доступ» устанавливает интервалы для всех дней от 00:00 до 23:59. Кнопка «Запрет» устанавливает интервалы для всех дней от 00:00 до 00:00.

Для редактирования выбранной группы доступа нужно выполнить двойной щелчок левой кнопкой мыши на соответствующей строке в списке групп доступа в окне «Настройка групп доступа и окон времени». При этом появляется окно «Группа доступа»:

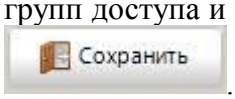


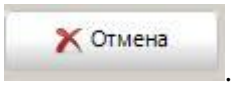
В этом окне можно указать «Название группы». В поле «Окна времени» выбираются необходимые для группы доступа окна времени. С помощью выпадающих списков «Окно 1», «Окно 2» и «Окно 3» можно выбрать до трёх окон времени.

В поле «Комбинация доступа» указывается способ аутентификации пользователя. Для выбора доступно 6 вариантов:

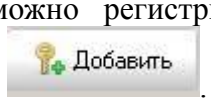
- отпечаток пальца
- Proximity карта
- пароль
- палец + карта
- палец + пароль
- палец + карта

В показанном на рисунке случае выбраны способы аутентификации «Proximity карта» и «Пароль». Это означает, что пользователь может получить доступ при предъявлении карты и пароля.

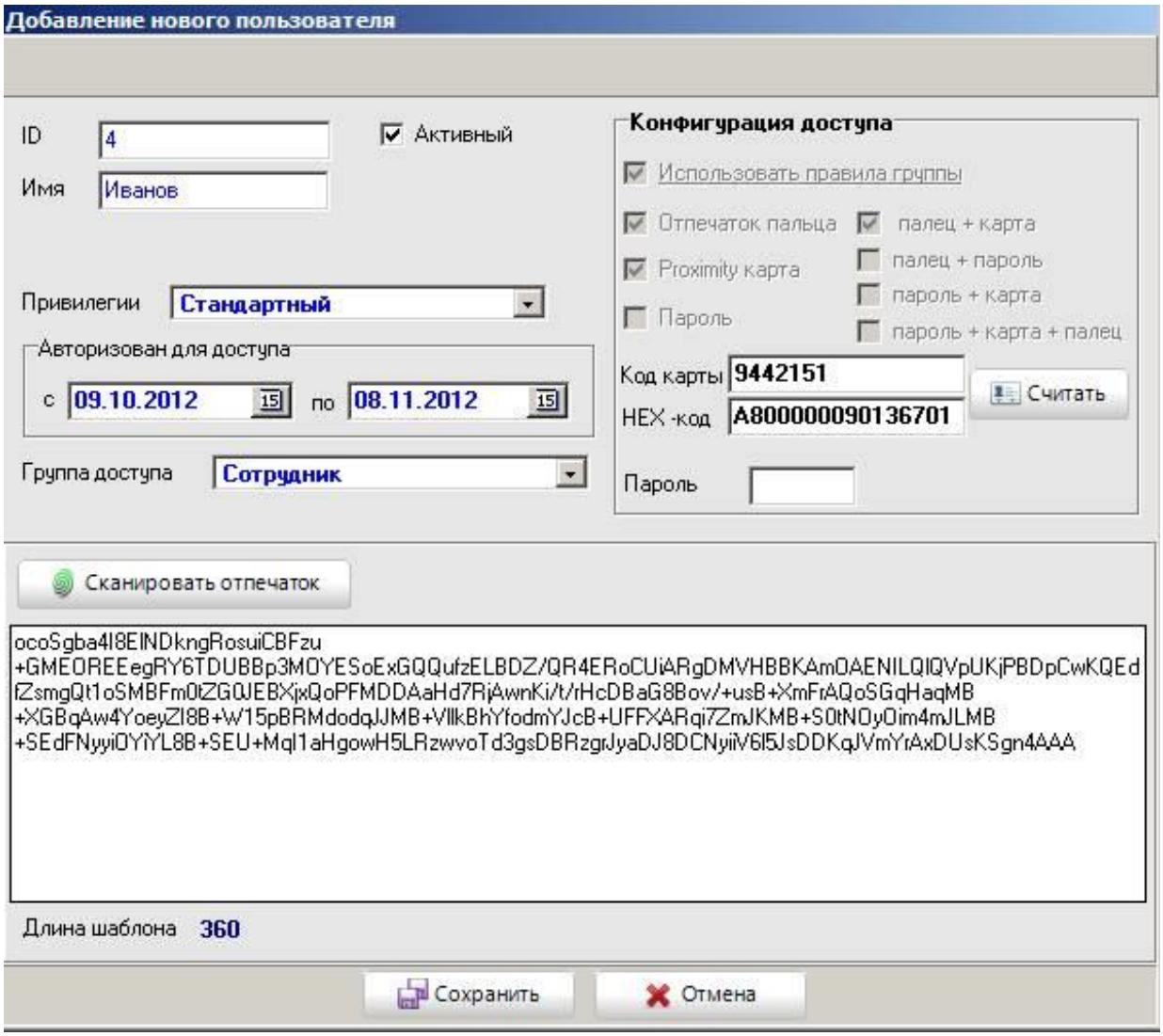
После завершения редактирования групп пользователей и временных окон в окне «Настройка групп доступа и окон времени» для сохранения введённых данных следует нажать на кнопку 

. Если сохранять данные не нужно, то следует нажать на кнопку 

.

После ввода нужных групп доступа и окон времени можно регистрировать новых пользователей. Для этого на вкладке «Доступ» нужно нажать 

. После нажатия на кнопку появляется окно «Добавление нового пользователя» (оно аналогично окну «Редактирование информации о пользователе»):



В этом окне указываются порядковый номер пользователя в общем списке пользователей (ID), имя пользователя (Имя). Имя должно содержать не более 8 символов. Опция «Активный» при отключении позволяет запретить доступ для зарегистрированного пользователя.

В списке «Привилегии» выбираются нужные привилегии по управлению контроллером. В BAProg можно предоставить пользователю полномочия администратора («Администратора») или обычного пользователя («Стандартный»).

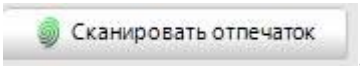
В поле «Авторизован для доступа» указывается интервал времени, в течение которого для пользователя сохраняется статус «Активный».

В списке «Группа доступа» выбирается необходимая группа доступа. Когда группа доступа выбрана, в поле «Конфигурация доступа» показываются настройки способа аутентификации для выбранной группы.

В зависимости от настроек способа аутентификации можно зарегистрировать код Proximity-карты, пароль или отпечаток пальца.

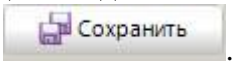
Для считывания кода карты нужно поднести карту к контроллеру и после этого нажать Считать. В полях «Код карты» и «HEX-код» появятся считанные значения.

Для регистрации пароля нужный пароль нужно ввести в поле «Пароль».

Для сканирования отпечатка пальца нужно нажать на кнопку 

. При этом появляется сообщение:

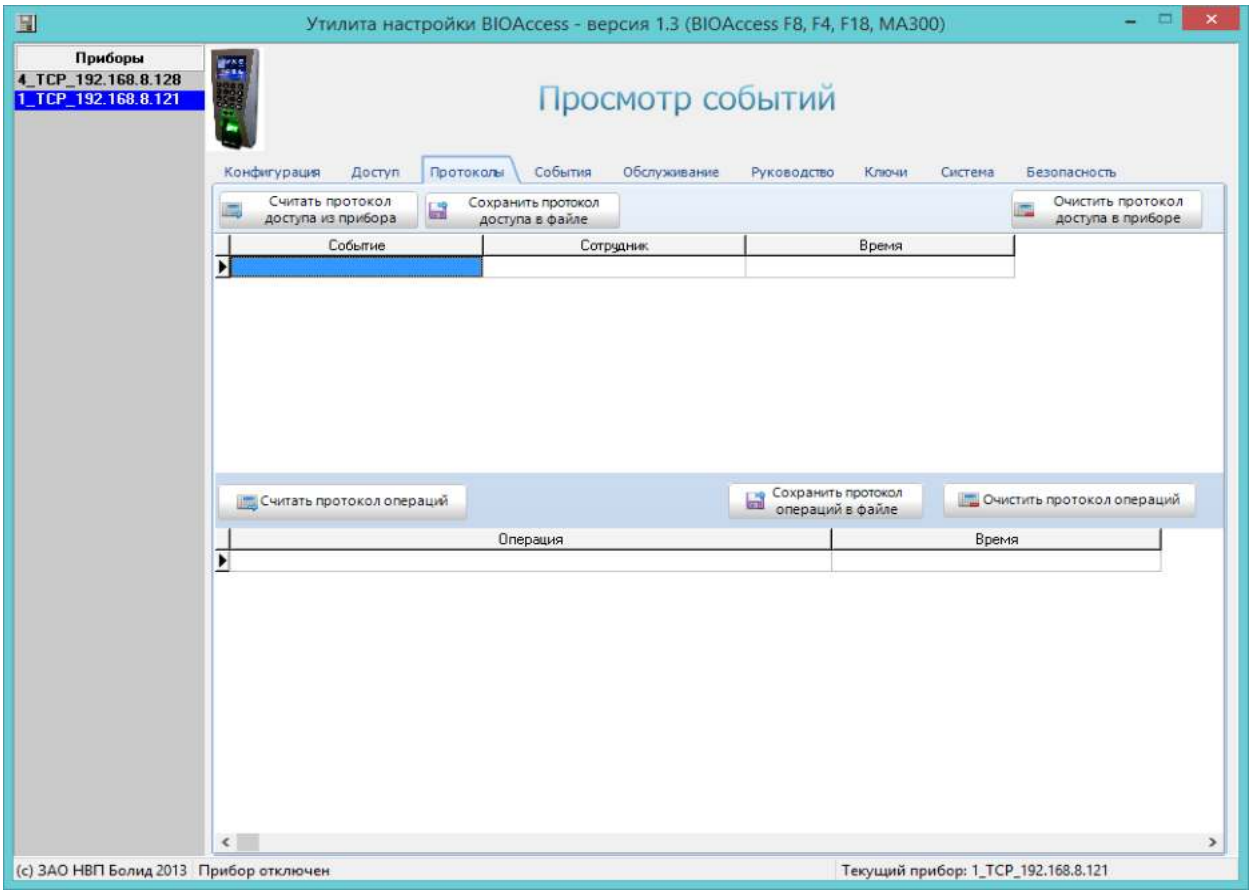
Для сканирования отпечатка нужно приложить нужный палец к сканеру три раза подряд. Если сканирование завершилось успешно, то в поле сканирования отпечатка пальца появится шаблон отпечатка пальца. Если отсканировать отпечаток не удалось, то поле останется пустым.

После ввода всех необходимых данных в окне «Добавление нового пользователя» для их сохранения нужно нажать 

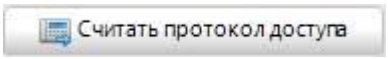
.

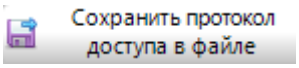
Вкладка «Протоколы прибора»

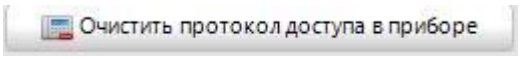
На этой вкладке можно просмотреть журнал доступа и журнал операций контроллера:

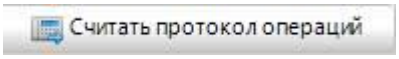


На этой вкладке расположены следующие кнопки:

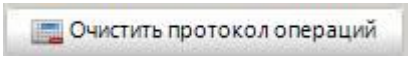
- 

– чтение из контроллера журнала доступа;
- 

- сохранение протокола доступа в текстовый файл;
- 

– очистка журнала доступа в контроллере;
- 

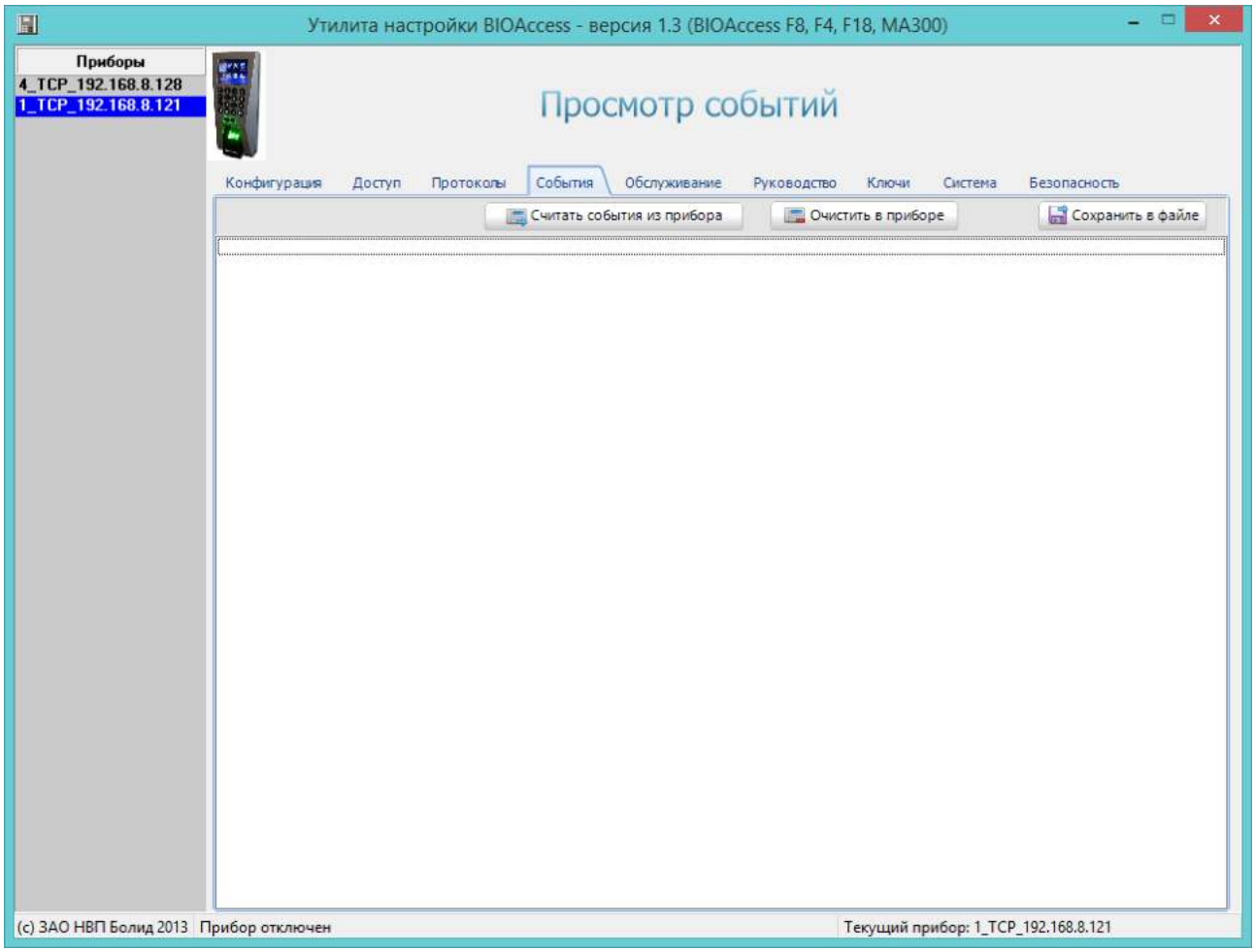
– чтение из контроллера журнала операций;
- 

– сохранение протокола операций в текстовый файл;
- 

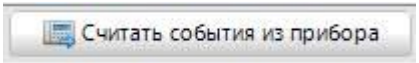
– очистка журнала операций в контроллере.

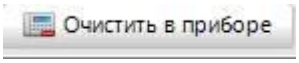
Вкладка «События»

На этой вкладке можно просмотреть журнал событий контроллера:

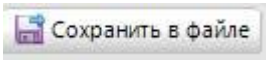


На этой вкладке расположены следующие кнопки:

- 

– чтение списка событий из контроллера;
- 

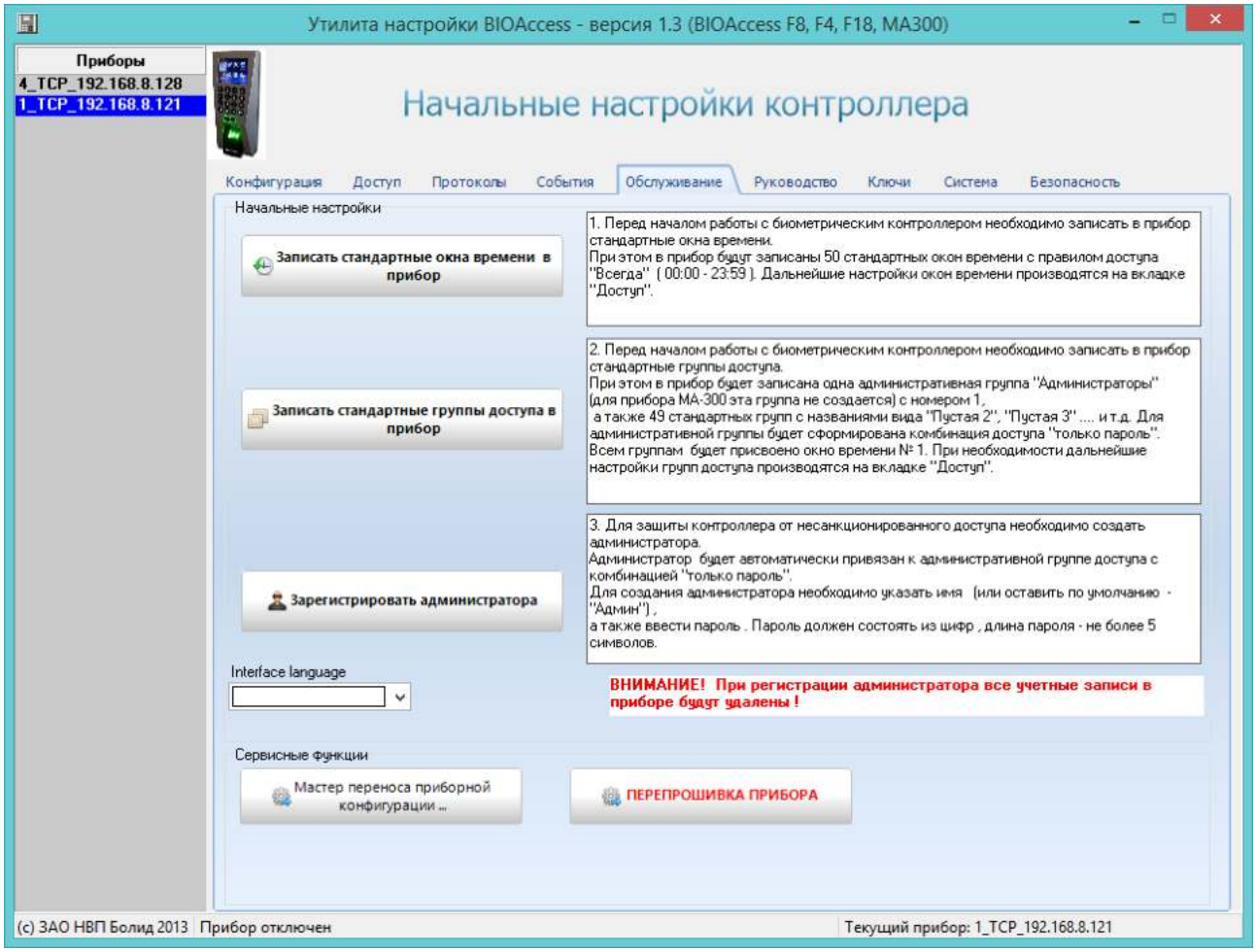
– очистка списка событий в контроллере;

- 

– сохранение списка событий в файле. При нажатии на эту кнопку открывается стандартный диалог Windows «Сохранить как», в котором можно указать нужное имя файла, в котором будет сохранён список событий контроллера.

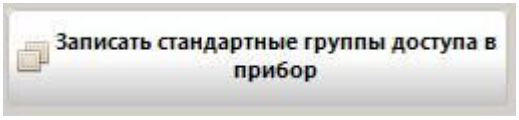
Вкладка «Обслуживание»

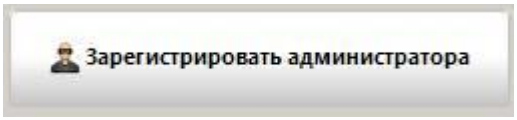
На этой вкладке осуществляются начальные настройки контроллера и сервисные функции.



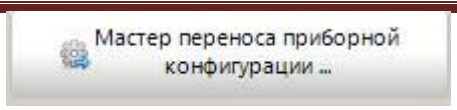
Начальные настройки контроллера осуществляются при нажатии на следующие кнопки:

- 

– создание в контроллере совместимых с «Орион Про» окон времени;
- 

– создание в контроллере совместимых с «Орион Про» групп доступа;
- 

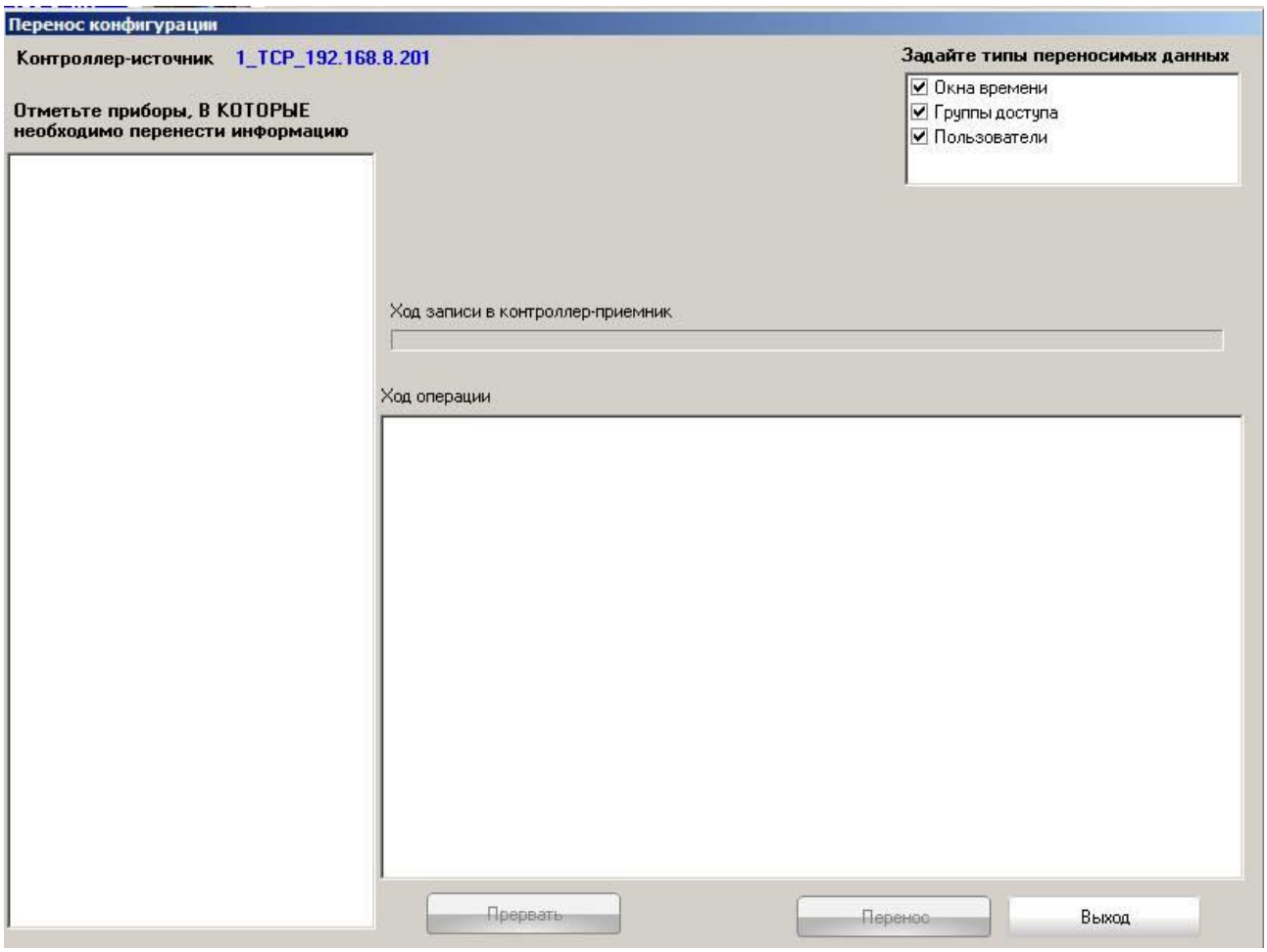
– регистрация в контроллере пользователя с правами администратора.

В поле «Сервисные функции» расположена кнопка 

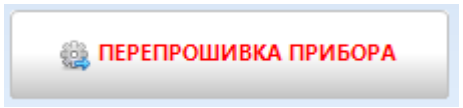
– копирование настроек контроллера в другой такой же контроллер. Используется для быстрой настройки нескольких контроллеров.

Мастер переноса приборной конфигурации

При нажатии на кнопку «Мастер переноса приборной конфигурации» появляется следующее окно:



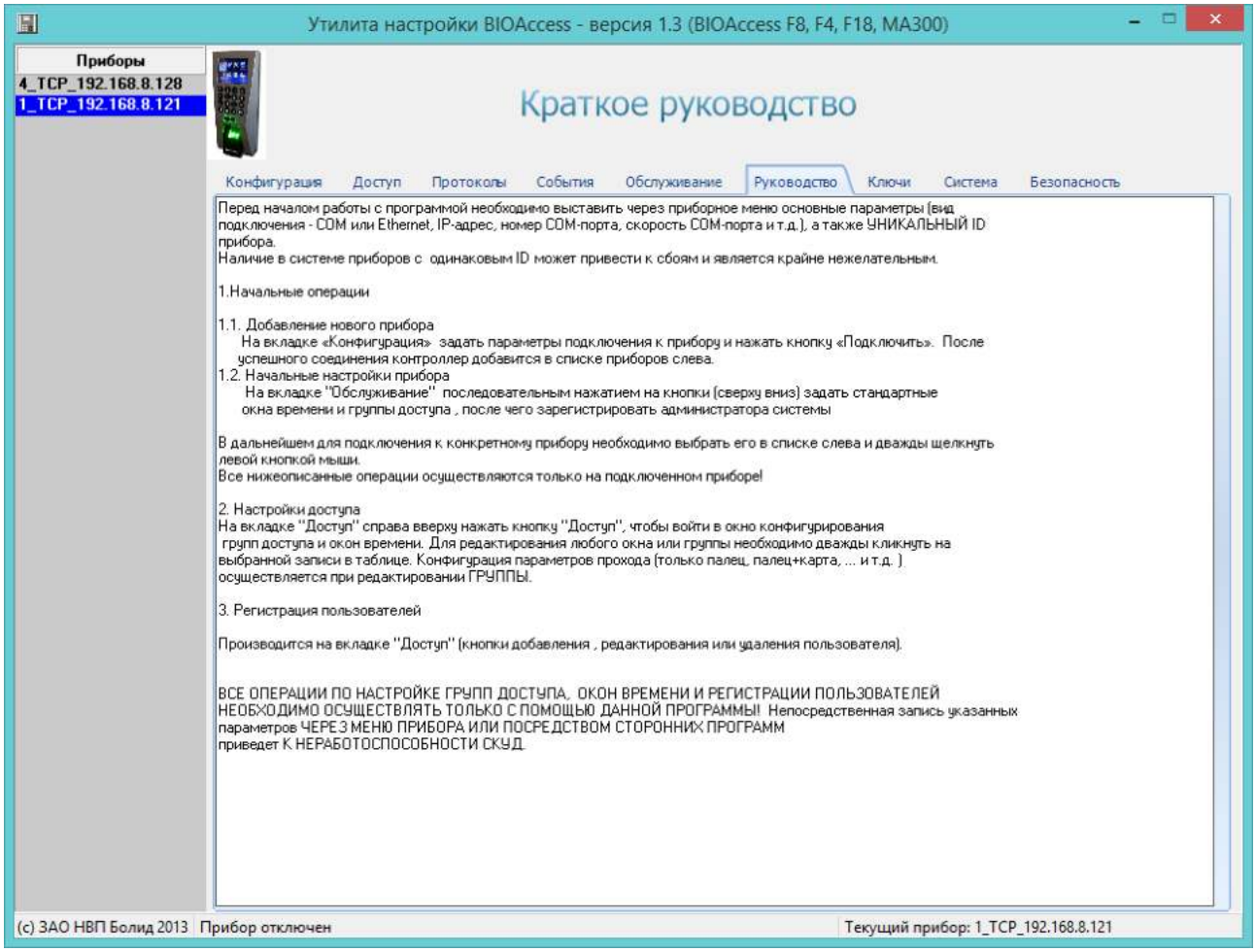
В этом окне в строке «Контроллер-источник» показано название контроллера, который выбран в BAProg в списке «Приборы» и который рассматривается в качестве источника при копировании конфигурационных данных. В левой части окна расположен список остальных подключённых приборов. В этом списке можно выбрать контроллеры, в которые должны быть скопированы данные. В правой верхней части окна можно указать, какие именно данные должны быть скопированы в другие контроллеры: окна времени; группы доступа; пользователи. Копирование начинается после нажатия на кнопку «Перенос». Процесс копирования можно прервать нажатием на кнопку «Прервать».



- обновление версии операционной системы контроллера в случае выпуска пакета обновлений для операционной системы.

Вкладка «Руководство»

На этой вкладке приводится краткое руководство по работе с контроллером в программе BAProg:

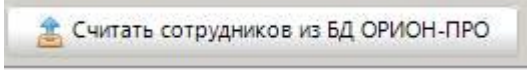


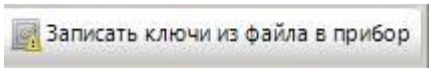
Вкладка «Ключи»

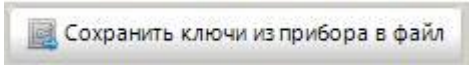
На этой вкладке осуществляется экспорт ключей из контроллера в базу данных «Орион Про».

Экспорт регистрационной информации в БД «Орион-Про» необходим в случаях, когда биометрические контроллеры в течение какого-то времени эксплуатировались в автономном режиме, без интеграции с ИСО «Орион-Про», и в эти контроллеры была записана регистрационная информация сотрудников (ID, имя, отпечаток пальца).

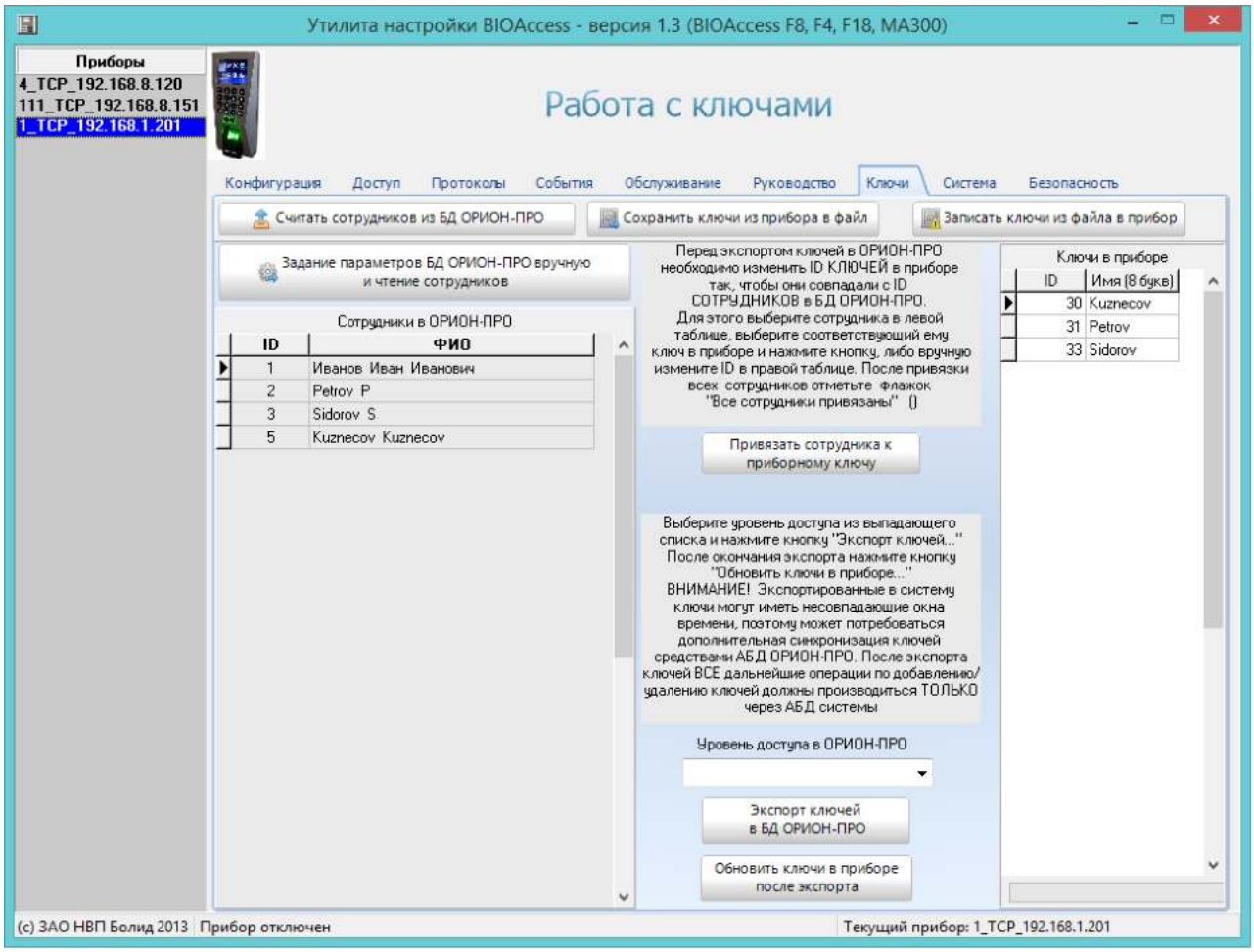
В верхней части вкладки расположены следующие кнопки:

- 

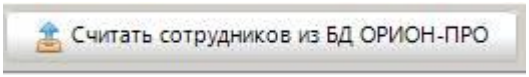
– загрузить список сотрудников из базы данных «Орион Про».
- 

– загрузить информацию о пользователях из файла в контроллер.
- 

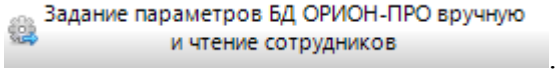
– сохранить информацию о пользователях, записанную в контроллере, в файл.



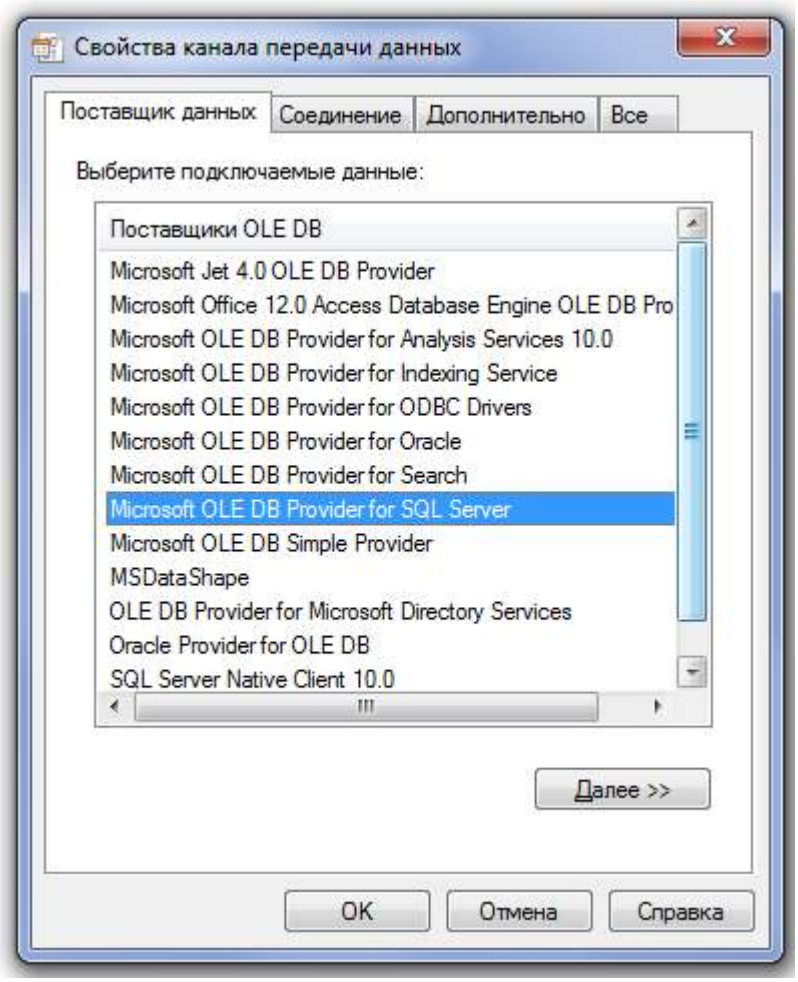
Ниже расположены списки сотрудников, считанные из базы данных «Орион Про» и из контроллера.

В левом столбце после нажатия на кнопку 

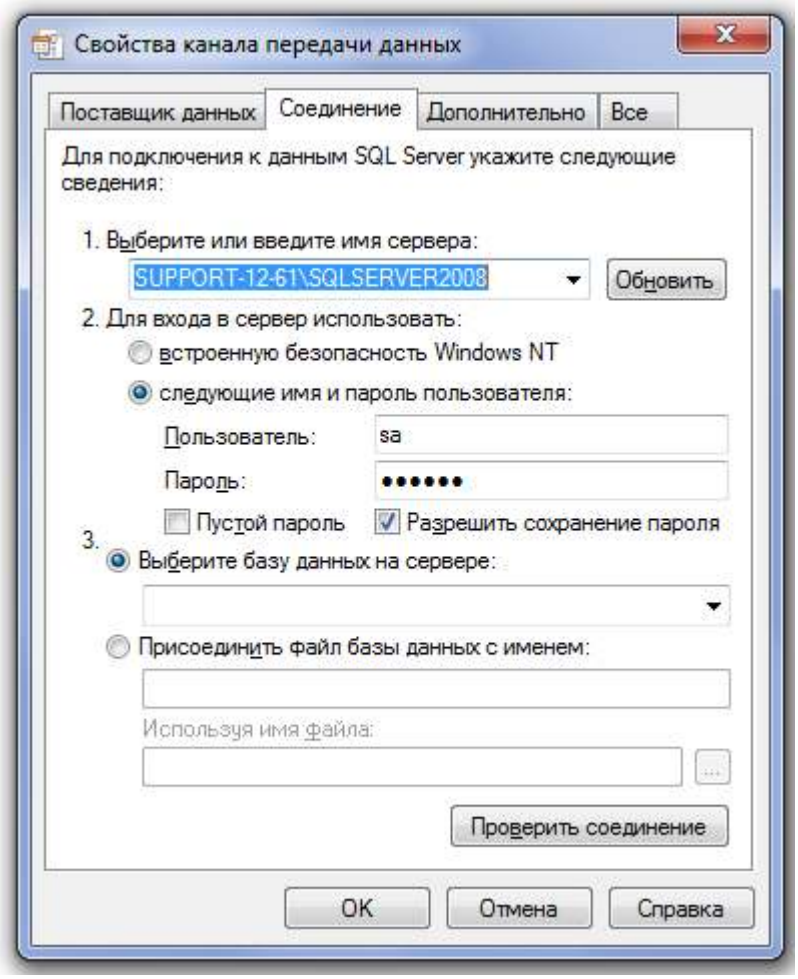
показывается список сотрудников, зарегистрированных в базе данных «Орион Про».

Если считать сотрудников из базы данных «Орион Про» не удается, то следует воспользоваться кнопкой 

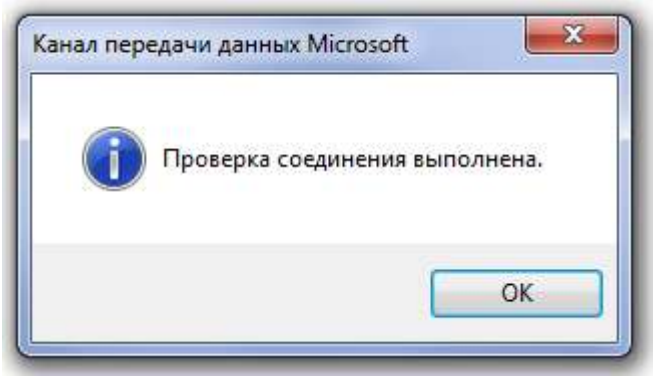
. При этом появляется окно «Свойства канала передачи данных».


Свойства канала передачи данных
Поставщик данных
Соединение
Дополнительно
Все
Выберите подключаемые данные:
Поставщики OLE DB
Microsoft Jet 4.0 OLE DB Provider
Microsoft Office 12.0 Access Database Engine OLE DB Pro
Microsoft OLE DB Provider for Analysis Services 10.0
Microsoft OLE DB Provider for Indexing Service
Microsoft OLE DB Provider for ODBC Drivers
Microsoft OLE DB Provider for Oracle
Microsoft OLE DB Provider for Search
Microsoft OLE DB Provider for SQL Server
Microsoft OLE DB Simple Provider
MSDataShape
OLE DB Provider for Microsoft Directory Services
Oracle Provider for OLE DB
SQL Server Native Client 10.0
Далее >>
OK
Отмена
Справка

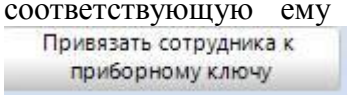
Во вкладке «Поставщик данных» следует выбрать строку «Microsoft OLE DB Provider for SQL server» и нажать кнопку Далее >>, произойдет перемещение на вкладку «Соединение».



Следует выбрать имя SQL-сервера из выпадающего списка или ввести вручную. Ввести имя пользователя и пароль администратора сервера «Орион-Про». Рекомендуется поставить галочку Разрешить сохранение пароля. После этого следует нажать кнопку Проверить соединение. При успешном соединении система выдаст следующее сообщение:

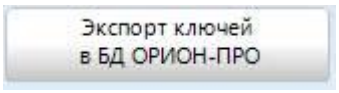


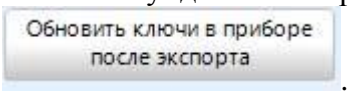
В случаи появления иного сообщения следует проверить введенные данные.

Перед экспортом ключей в «Орион Про» необходимо изменить номера (ID) ключей в контроллере так, чтобы они совпадали с ID сотрудников в базе данных «Орион Про». Для этого нужно выбрать сотрудника в списке «Сотрудники в ОРИОН-ПРО», выбрать соответствующую ему запись в списке «Ключи в приборе» и нажать на кнопку 

. Также можно назначить нужный номер, выполнив двойной щелчок левой кнопкой мыши на изменяемом номере.

После согласования списков между собой нужно отметить поле «Все сотрудники привязаны». При этом ниже появятся список уровней доступа и две кнопки. В списке «Уровень доступа в ОРИОН-ПРО» нужно выбрать нужный уровень доступа для пользователей.

После нажатия на кнопку 

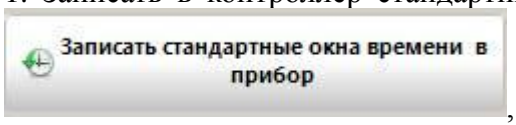
осуществляется экспорт информации о сотрудниках в базу данных «Орион Про». После завершения экспорта нужно нажать на кнопку 

.

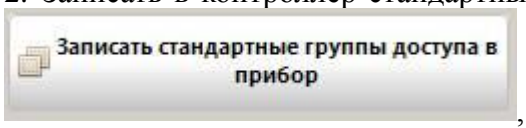
Экспортированные в систему ключи могут иметь несовпадающие окна времени, поэтому может потребоваться дополнительная синхронизация ключей средствами Администратора Базы Данных «Орион Про».

Начальная настройка контроллера

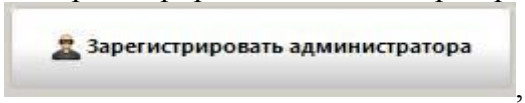
Для того чтобы контроллер можно было использовать в АРМ «Орион Про», необходимо на вкладке «Обслуживание» программы BAProg выполнить следующие операции:

1. Записать в контроллер стандартные окна времени. Для этого нужно нажать на кнопку 

, в появившемся окне подтвердить выполнение операции (нажать на кнопку «ОК»). При этом в контроллер будут записаны 50 стандартных окон времени с правилом доступа «Всегда» (00:00-23:59).

2. Записать в контроллер стандартные группы доступа. Для этого нужно нажать на кнопку 

, в появившемся окне подтвердить выполнение операции (нажать на кнопку «ОК»). При этом в контроллер будет записана одна административная группа «Администраторы» с номером 1, а также 49 стандартных групп с названиями вида «Пустая 2», «Пустая 3» и т. д. Для административной группы будет сформирована комбинация доступа «только пароль». Всем группам будет присвоено окно времени №1.

3. Зарегистрировать администратора контроллера. Для этого нужно нажать на кнопку 

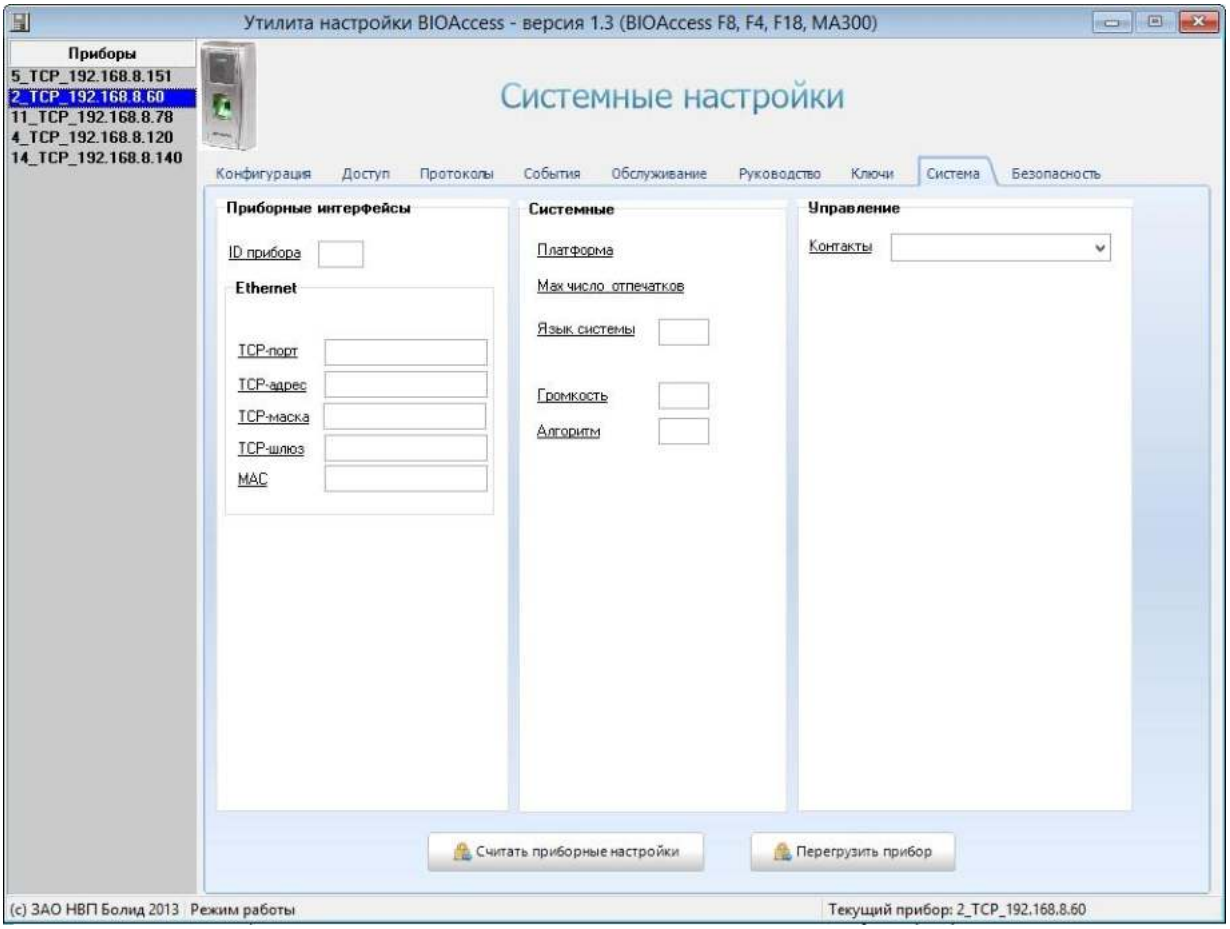
, в появившемся запросе подтвердить выполнение операции (нажать на кнопку «Да»). Администратор будет автоматически привязан к административной группе доступа с комбинацией «только пароль». Для создания администратора необходимо указать имя (или оставить по умолчанию – «Админ»), а также ввести пароль. Пароль должен состоять из цифр, длина пароля – не более 5 символов. При регистрации администратора все остальные учётные записи в контроллере будут удалены!

После выполнения перечисленных операций нужно отключить электропитание от контроллера, а затем снова подключить. Это необходимо для того, чтобы произведённые настройки вступили в силу.

Вкладка «Система»

Данная вкладка является вспомогательной, и предназначена для получения дополнительной информации о контроллере, а также для «тонкой» настройки системы. Как правило, использование данной вкладки бывает необходимо в процессе технических консультаций, при возникновении у пользователя вопросов по работе с контроллером.

Категорически не рекомендуется работать с данной вкладкой без явного указания и/или запроса от технического консультанта компании «Болид»



Вкладка «Безопасность»

Данная вкладка предназначена для задания параметров защищенного режима (ЗР). Этот режим реализован только в контроллерах С2000-BIOAccess-MA300.

Защищенный режим (ЗР) предотвращает возможность несанкционированного доступа в помещение (путём отрыва прибора от стены и замыкания контактов реле вручную).

В этом режиме замок двери управляется контроллером С2000-2 или С2000-4, к которому в качестве Wiegand-считывателя подключается биометрический контроллер.

Для этого следует подключить контакты WD0-OUT и WD1-OUT разъёма J6 контроллера к соответствующим контактам контроллера доступа С2000-2. Замок следует подключать к контроллеру доступа С2000-2.

Подробнее подключение внешних цепей к контроллеру доступа С2000-2 описано в руководстве по эксплуатации данного контроллера.

Принцип работы режима ЗР следующий. После успешной верификации отпечатка пальца (или любой комбинации типа только карта, палец+карта) биометрический контроллер выдаёт по интерфейсу Wiegand код «секретной карты» в контроллер С2000-2, и контроллер С2000-2, проверив полномочия «секретной карты», открывает дверь. Поскольку реле биометрического контроллера в этом режиме не подключены к замку, то тем самым и гарантируется защита от проникновения в охраняемое помещение.

Для реализации ЗР необходимо:

1. Подключить биометрический контроллер к компьютеру и через программу BAProg задать ID и код Proximity-карты («секретной» карты);

2. Включить режим ЗР;

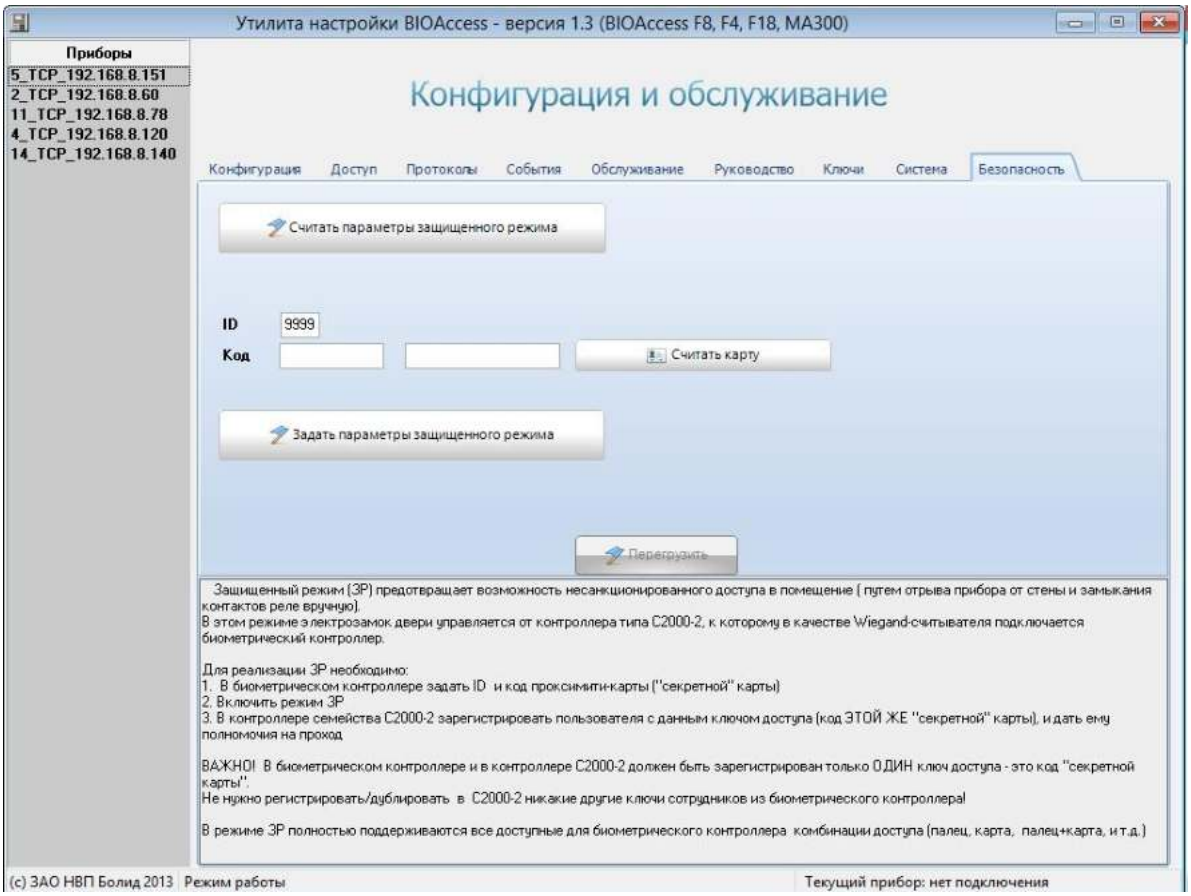
3. В контроллере С2000-2 зарегистрировать пользователя с данным ключом доступа (код ЭТОЙ ЖЕ «секретной» карты), и дать ему полномочия на проход.

В контроллере С2000-2 должен быть зарегистрирован только ОДИН ключ доступа – это код «секретной карты».

Не нужно регистрировать/дублировать в С2000-2 никакие другие ключи сотрудников из биометрического контроллера.

В режиме ЗР полностью поддерживаются все доступные для биометрического контроллера комбинации доступа (палец, карта, палец+карта, и т.д.).

В качестве «секретной карты» можно использовать карту, идущую в комплекте поставки.



Кнопка «Считать параметры защищенного режима» позволяет принудительно считать из прибора и отобразить текущие настройки ЗР.

Перед включением защищенного режима необходимо соединить биометрический контроллер с контроллером типа С2000-2. Для этого выходы Wiegand WD1-OUT (белый провод) и WD0-OUT (зеленый провод) необходимо подключить к входам Wiegand D1-1 и D0-1 контроллера С2000-2 соответственно. Таким образом, в данном режиме биометрический контроллер используется контроллером С2000-2 в качестве считывателя Proximity-карт.

Для включения режима необходимо в поле «Код» ввести код Proximity-карты («секретной карты»). Это может быть сделано вручную, либо путем считывания кода Proximity-карты по кнопке «Считать карту». В поле ID необходимо ввести любое число от 1 до 32765, (рекомендуется вводить число типа 9999 или 8888). Далее, по нажатию кнопки «Задать параметры защищенного режима», производится запись указанных параметров в биометрический контроллер, после чего прибор необходимо перегрузить.

«Секретную карту» рекомендуется хранить в защищенном от посторонних лиц месте, кроме того, целесообразно периодически обновлять «секретную карту», путем регистрации в биометрическом контроллере и в контроллере С2000-2 кода другой Proximity-карты.