



EAC

Биометрический контроллер доступа

C2000-BIOAccess-MA300

Руководство пользователя

Настоящее руководство пользователя предназначено для изучения принципов работы и эксплуатации биометрического контроллера доступа «С2000-ВІОAccess-МА300».

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;

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

Содержание

Общие сведения	4
Меры предосторожности	5
Получение качественных изображений отпечатков пальцев	5
Внешний вид, органы управления	6
Основные технические данные	8
Подготовка к эксплуатации	8
Комплект поставки	9
Монтаж контроллера	9
Схемы электрических соединений	10
Подключение к контроллеру периферийного оборудования	12
Автономная работа	13
Подключение к ПК	13
ВАProg	15
Установка ВАProg	15
Интерфейс ВАProg	20
Вкладка «Конфигурация»	21
Вкладка «Доступ»	23
Вкладка «Протоколы»	30
Вкладка «События»	31
Вкладка «Обслуживание»	32
Вкладка «Руководство»	34
Вкладка «Ключи»	34
Вкладка «Система»	36
Вкладка «Безопасность»	37
Начальная настройка контроллера	38
<i>Настройка сетевых параметров</i>	38
<i>Настройка параметров доступа</i>	40
Настройка контроллера в ВАProg	41
Обслуживание	41
Гарантии изготовителя (поставщика)	42
Сведения о сертификации	42

Общие сведения

Биометрический контроллер доступа «С2000-ВIOAccess-МА300» (далее – контроллер) предназначен для совместной работы с АРМ «Орион Про» для организации системы контроля и управления доступом (СКУД) по биометрическим идентификаторам – отпечаткам пальцев.

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

Контроллер обеспечивает световую и звуковую индикацию своего состояния.

Контроллер может работать под управлением персонального компьютера или в автономном режиме. Контроллер соединяется с ПК через Ethernet (TCP/IP). Наличие высокоскоростного интерфейса Ethernet позволяет использовать для подключения уже имеющиеся локальные сети (LAN), без прокладки дополнительных магистралей.

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

В контроллере предусмотрен режим мультиидентификации – предоставление доступа по комбинации двух идентификаторов отпечаток пальца и Proximity-карточка.

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

Контроллер оборудован датчиком вскрытия корпуса. При изменении состояния датчика контроллер передаёт управляющему ПК соответствующие сообщения.

Энергонезависимая память служит для хранения значений конфигурационных параметров контроллера, информации о пользователях и журналов событий.

Настройка контроллера «С2000-ВIOAccess-МА300» выполняется с помощью программы конфигурирования биометрических контроллеров ВАProg. Новейшую версию программы ВАProg можно скачать с сайта компании «Болид» по адресу <http://bolid.ru> в разделе «Продукция».

Электропитание контроллера осуществляется с помощью 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 падение брызг воды в любом направлении (степень защиты оболочки IP54). Конструкция контроллера не предусматривает его использование в условиях воздействия агрессивных сред, а также во взрывопожароопасных помещениях. Контроллер относится к невосстанавливаемым, периодически обслуживаемым изделиям.

Меры предосторожности

ВНИМАНИЕ! Для связи контроллеров с компьютером и между собой следует использовать сеть Ethernet.

ПРИ РАБОТЕ В СКУД ВСЕ ОПЕРАЦИИ ПО НАСТРОЙКЕ ГРУПП ДОСТУПА, ОКОН ВРЕМЕНИ И РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЕЙ НЕОБХОДИМО ОСУЩЕСТВЛЯТЬ ТОЛЬКО С ПОМОЩЬЮ ПРОГРАММЫ VAPROG! Запись указанных параметров ПОСРЕДСТВОМ СТОРОННИХ ПРОГРАММ приведёт К НЕРАБОТОСПОСОБНОСТИ СКУД.

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

Диапазон рабочих температур контроллера: от -10 до 60 °С. Не используйте контроллер при высокой температуре окружающей среды. Не подвергайте контроллер воздействию источников тепла и обеспечивайте адекватную вентиляцию контроллера, чтобы уменьшить риск перегрева.

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.

Получение качественных изображений отпечатков пальцев

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

Алгоритм получения отпечатка пальца часто 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:

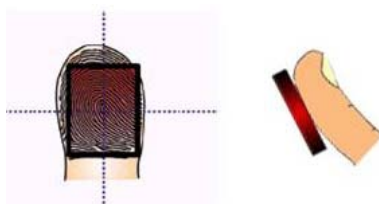


Рисунок 1. Правильное положение пальца при сканировании

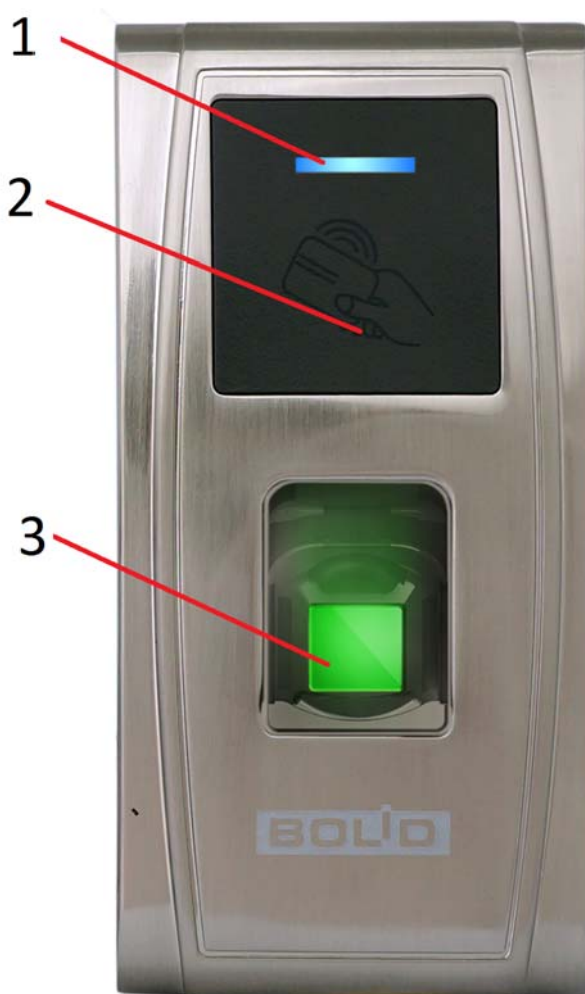
Внешний вид, органы управления

Рисунок 2. Лицевая панель «С2000-ВIOAccess-F18»

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

- 1) светодиодный индикатор
- 2) считыватель Proximity-карт
- 3) считыватель отпечатков пальцев

Светодиодный индикатор может работать в нескольких режимах, перечисленных в следующей таблице:

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 1 с	Ошибка аутентификации
Загорается зелёный светодиод на 1 с	Успешная верификация

Внутри корпуса, под наклейкой с изображением карточки, расположена антенна считывателя Proximity-карт.

С нижней стороны контроллера находится кнопка «Reset», позволяющая перезагрузить контроллер. Здесь же находятся разъём для подключения USB-накопителя (через переходник Mini-USB-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.

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
➤ Объём буфера событий, записей	100 000
➤ Диапазон температур, °С	от -10 до +60
➤ Относительная влажность воздуха, %	от 10 до 90
➤ Степень защиты оболочки	IP54
➤ Габаритные размеры, мм	не более 73×148×34,5
➤ Масса, кг	не более 1

Подготовка к эксплуатации

Перед использованием контроллера нужно удалить защитную плёнку со считывателя отпечатков пальцев.

Для проверки работоспособности контроллера необходимо выполнить следующую последовательность действий:

1. Подать питание на контроллер.
2. Включается подсветка считывателя отпечатков пальцев. Светодиодный индикатор выключен.
3. В течение 1 мин после включения питания контроллер должен перейти в рабочий режим. При этом контроллер воспроизведет сообщение «Режим идентификации. Пожалуйста, приложите палец или поднесите карту»; светодиодный индикатор мигает зеленым цветом с частотой 0,5 Гц.
4. Подключить контроллер к ПК через интерфейс Ethernet и подключиться к нему с помощью программы VARprog. Подробнее подключение контроллера в ПК и работа с программой VARprog описаны в соответствующих разделах настоящего руководства.

Для проверки работы системы доступа следует зарегистрировать в системе отпечаток тестового пользователя, назначить права доступа. Затем проверить правильность предоставления доступа. По завершении проверки запись тестового пользователя следует удалить из базы. Регистрация тестового пользователя осуществляется с помощью программы «VARprog» (см. далее).

Комплект поставки

В комплект поставки «C2000-BIOAccess-MA300» входят:

- «C2000-BIOAccess-MA300» – 1 шт.
- Паспорт – 1 экз.
- Инструкция по монтажу – 1 экз.
- Шаблон разметки для монтажа – 1 шт.
- Провода с разъёмами – 3 шт.
- Переходник Mini-USB-USB – 1 шт.
- Кронштейн – 1 шт.
- Винт для фиксации на кронштейне – 2 шт.
- Шуруп для крепления кронштейна – 4 шт.
- Отвёртка «звёздочка» T10 – 1 шт.
- Диод FR 107 – 1 шт.
- DVD-диск с ПО – 1 шт.
- Proximity-карточка – 1 шт.

Монтаж контроллера

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

ВНИМАНИЕ! Для закрепления контроллера на кронштейне используются винты под отвёртку T10 «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 необходимо удалить защитную плёнку со сканера отпечатков пальцев. При наклеенной защитной плёнке на сканере отпечатков пальцев не гарантируется их корректное распознавание.

Схемы электрических соединений

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

Разъем питания – однорядный разъем, 2 контакта;

Основной разъем – двухрядный разъем, 10 контактов;

Разъем Ethernet – стандартный разъем RJ45;

Разъем Wiegand – однорядный разъем, 6 контактов, не используется в данной версии.

Таблица 2. Назначение и описание контактов разъема 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
8	485+*	RS485 А, сиреневый
9	NO1	Реле замка, нормально-разомкнутый контакт, синий
10	485-*	RS485 В, коричневый

* – неиспользуемые в текущей версии контроллера контакты

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
3	GND*	Питание внешнего считывателя - GND, черный
4	WD0-IN*	Внешний считыватель – Wiegand – данные «0», зеленый
5	WD1-IN*	Внешний считыватель – Wiegand – данные «1», белый
6	+12V-OUT*	Питание внешнего считывателя - +12 В, красный

* – неиспользуемые в текущей версии контроллера контакты

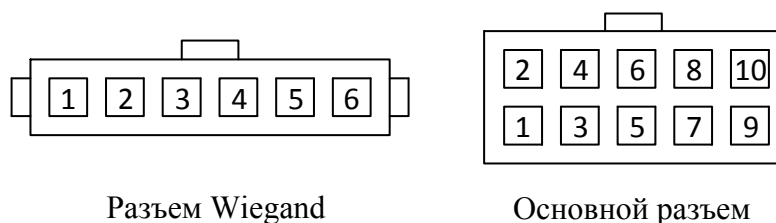


Рисунок 3. Нумерация контактов разъемов контроллера

В первую очередь необходимо подсоединять провод выравнивания потенциалов (GND), что позволит предотвратить электростатическое повреждение контроллера.

Провод электропитания следует подсоединять к контроллеру в последнюю очередь. Если контроллер работает с нарушениями, то перед проверкой/демонтажем необходимо отключать электропитание. **Подсоединение проводов к контроллеру при включённом электропитании может привести к повреждению контроллера.**

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

Подключение к контроллеру периферийного оборудования

Датчик двери используется для определения положения двери (открыта/закрыта). Контроллер может выявлять несанкционированный проход через дверь и включать сигнал тревоги, если дверь была открыта неавторизованным пользователем или открыта слишком долго.

К контроллеру можно подсоединять звуковые оповещатели с напряжением электропитания 12 В.

Электрический замок не должен питаться от того же источника питания, что и контроллер. **Необходимо питать электрические замки от отдельного источника питания.** Если в конструкции замка не предусмотрена схема подавления импульсов высокого напряжения, возникающих при коммутации питания, то 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. **Установка диода обязательна, даже в случае питания замка от отдельного источника.** На рис. 4 приведены рекомендуемые схемы подключения замков.

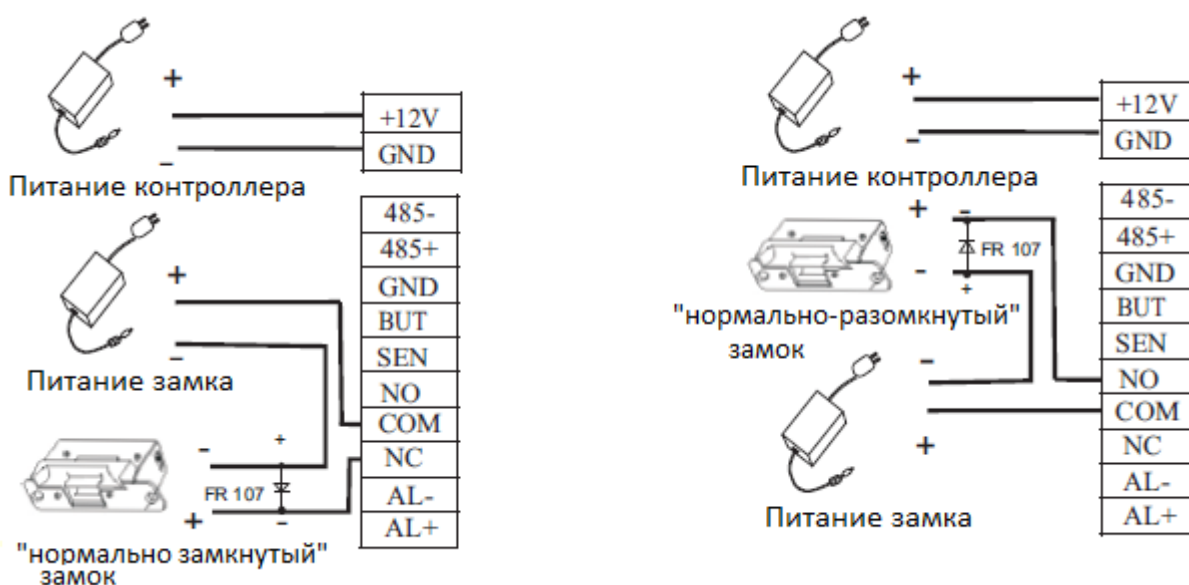


Рисунок 4. Рекомендуемые схемы подключения замков

Для организации защищенного режима работы контроллер по интерфейсу Wiegand-26 подключается к контроллеру доступа «С2000-2», который будет управлять замком. Для этого следует подключить контакты WD0-OUT и WD1-OUT разъема 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.

Автономная работа

При использовании контроллера в автономном режиме (без ИСО ОРИОН-ПРО) настройку требуется выполнять в программе ВАРprog.

После настройки в ВАРprog (см. далее) контроллер может использоваться в качестве автономного контроллера доступа.

В случае использования контроллера в качестве автономного контроллера доступа рекомендуется создавать резервную копию шаблонов отпечатков пальцев, например, на жёстком диске ПК или на другом накопителе информации. Это поможет при возможном сбое в работе контроллера быстро восстановить базу данных отпечатков пальцев, не прибегая к полному повторному сканированию.

Подключение к ПК

ВНИМАНИЕ! Для связи контроллеров с компьютером и между собой следует использовать сеть Ethernet.

На рис. 5, 6 приведены схемы подключения контроллеров по интерфейсу Ethernet.

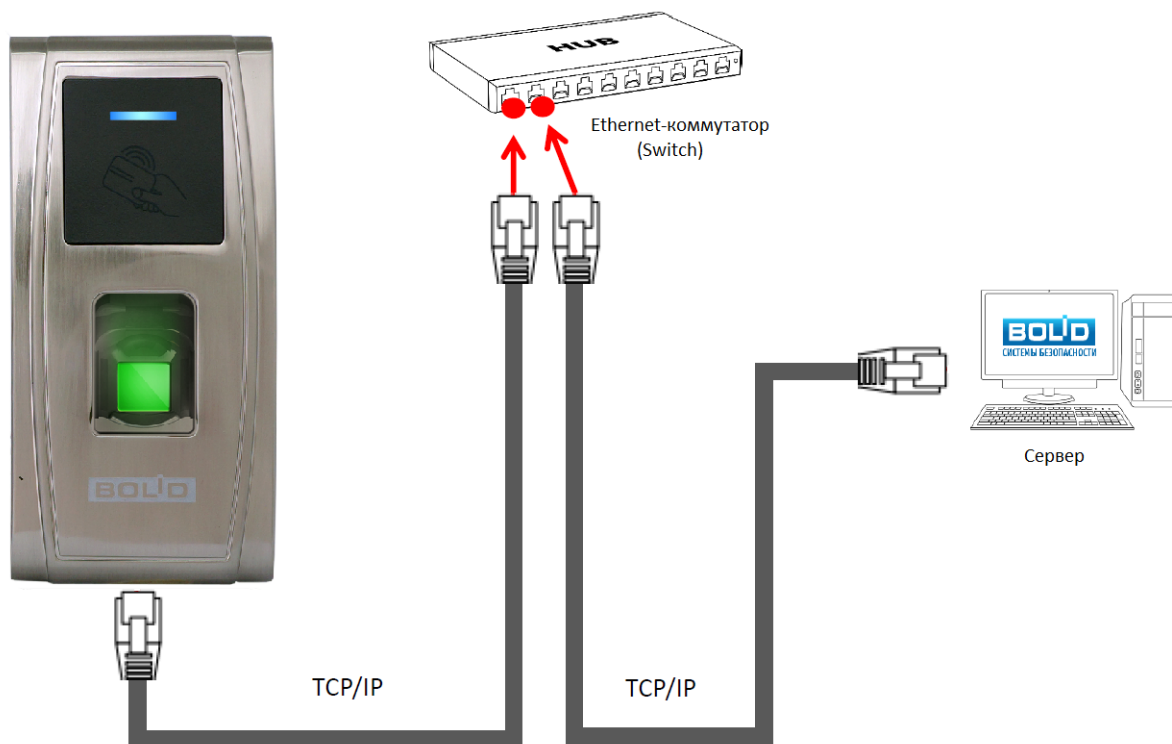


Рисунок 5. Подключение контроллера к ПК через Ethernet-коммутатор (Switch)

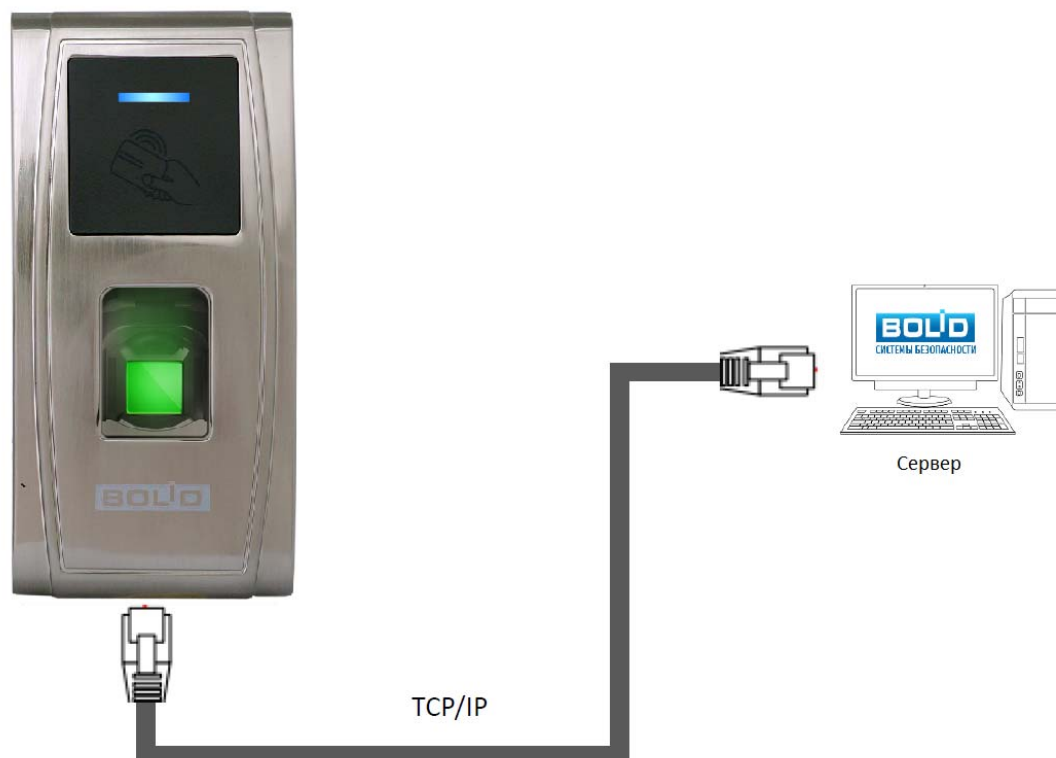


Рисунок 6. Подключение контроллера к ПК напрямую

При подключении контроллера непосредственно к компьютеру используется crossover-кабель.

При подключении по Ethernet каждому контроллеру назначается IP-адрес.

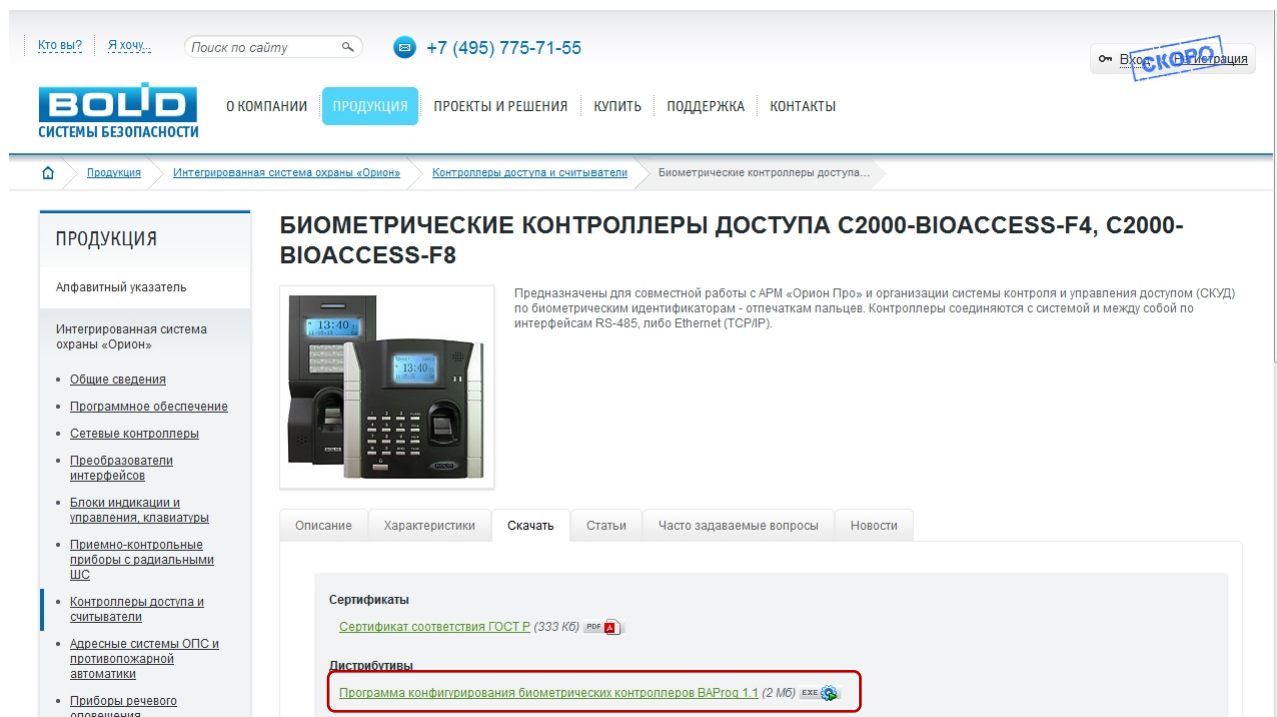
Если для подключения контроллеров используется сеть Ethernet, то можно сразу подключить все контроллеры в сеть.

ВАProg

Программа ВАProg используется для конфигурирования «C2000-BIOAccess-F4».

Установка ВАProg

Новейшую версию программы ВАProg можно скачать с сайта <http://bolid.ru> со страницы <http://bolid.ru/production/orion/access-controller/s2000-bioaccess.html?tab=download>.



The screenshot shows the BOLID website interface. At the top, there is a search bar and a phone number: +7 (495) 775-71-55. The main navigation menu includes 'ПРОДУКЦИЯ', 'ПРОЕКТЫ И РЕШЕНИЯ', 'КУПИТЬ', 'ПОДДЕРЖКА', and 'КОНТАКТЫ'. The breadcrumb trail indicates the current page is 'Биометрические контроллеры доступа...'. The main content area is titled 'БИОМЕТРИЧЕСКИЕ КОНТРОЛЛЕРЫ ДОСТУПА С2000-BIOACCESS-F4, С2000-BIOACCESS-F8'. Below the title, there is an image of the access controller and a description: 'Предназначены для совместной работы с АРМ «Орион Про» и организации системы контроля и управления доступом (СКУД) по биометрическим идентификаторам - отпечаткам пальцев. Контроллеры соединяются с системой и между собой по интерфейсам RS-485, либо Ethernet (TCP/IP)'. Below the description, there are tabs for 'Описание', 'Характеристики', 'Скачать', 'Статьи', 'Часто задаваемые вопросы', and 'Новости'. Under the 'Скачать' tab, there is a section for 'Сертификаты' with a link to 'Сертификат соответствия ГОСТ Р (333 Кб) pdf' and a section for 'Дистрибутивы' with a link to 'Программа конфигурирования биометрических контроллеров ВАProg 1.1 (2 Мб) exe' highlighted with a red box.

Рисунок 7

Минимальные системные требования ВАProg:

- 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 или Windows 7.

ВАProg предоставляется в виде установочного файла с расширением .exe. При запуске программы установки появляется следующее окно:

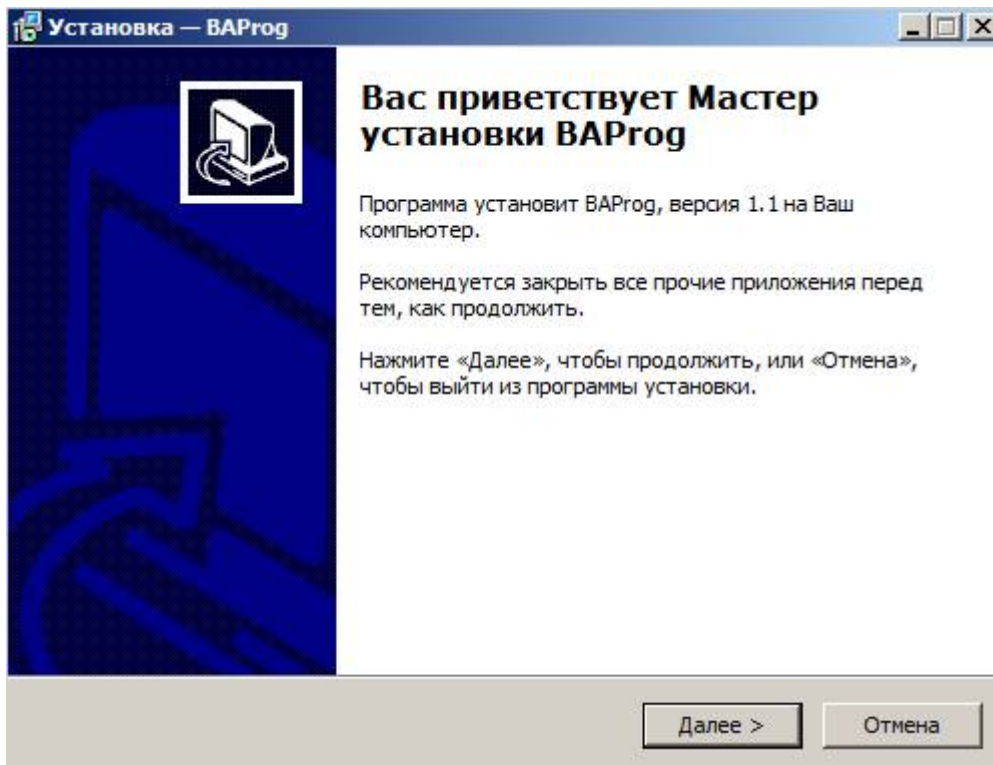


Рисунок 8

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

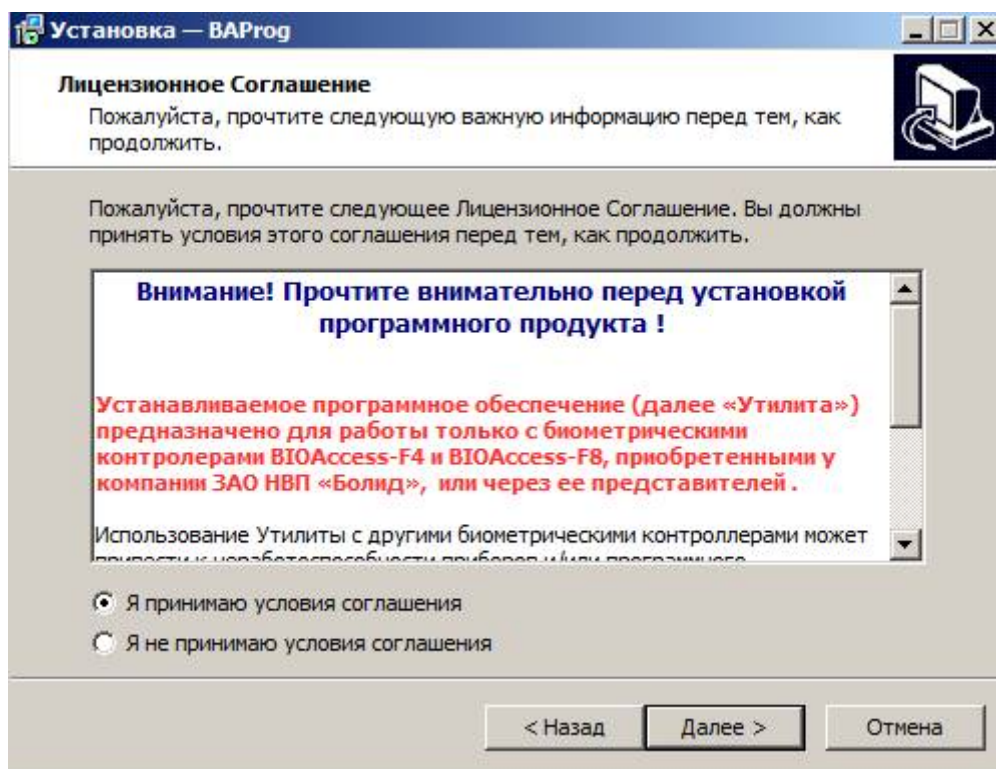


Рисунок 9

C2000-BIOAccess-MA300

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

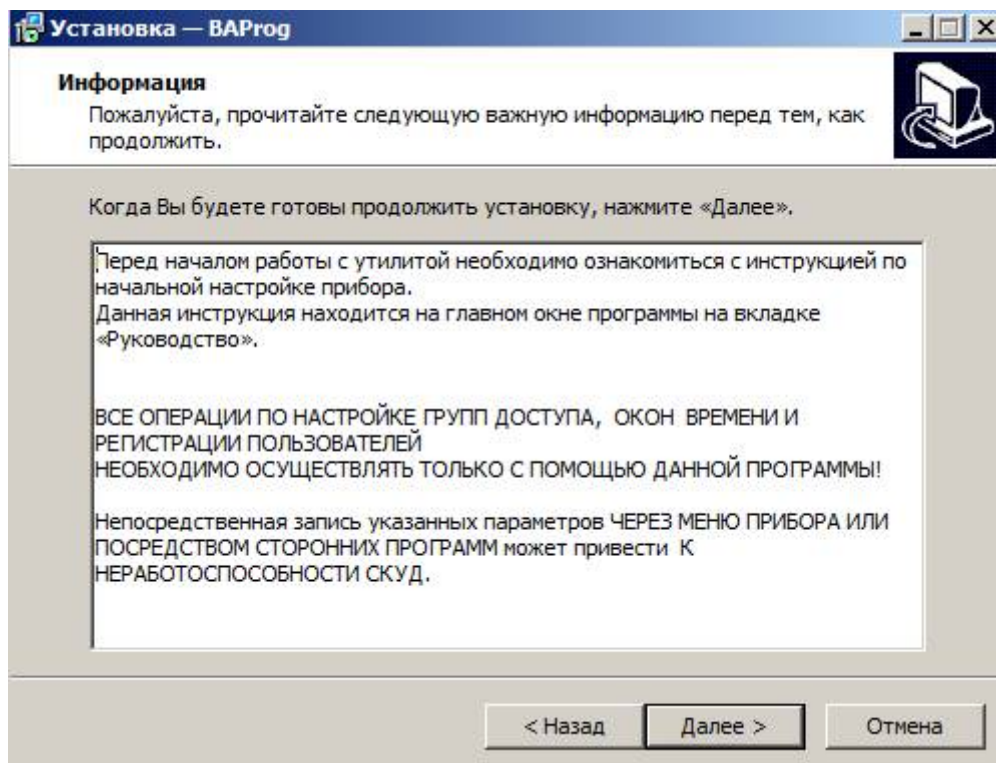


Рисунок 10

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

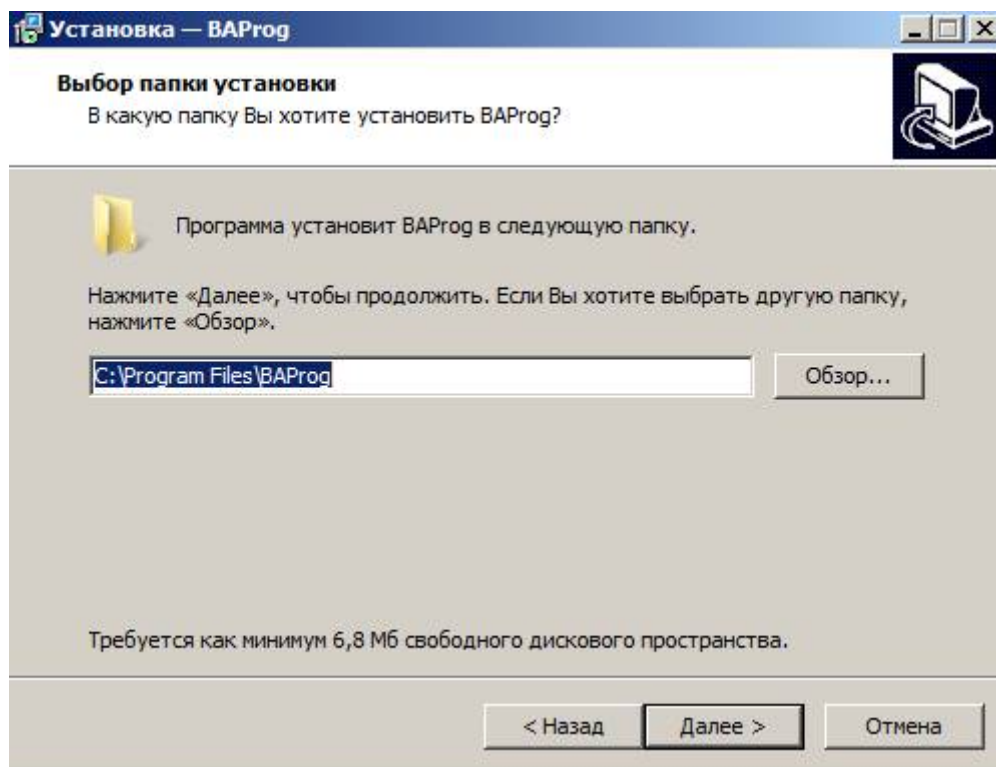


Рисунок 11

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

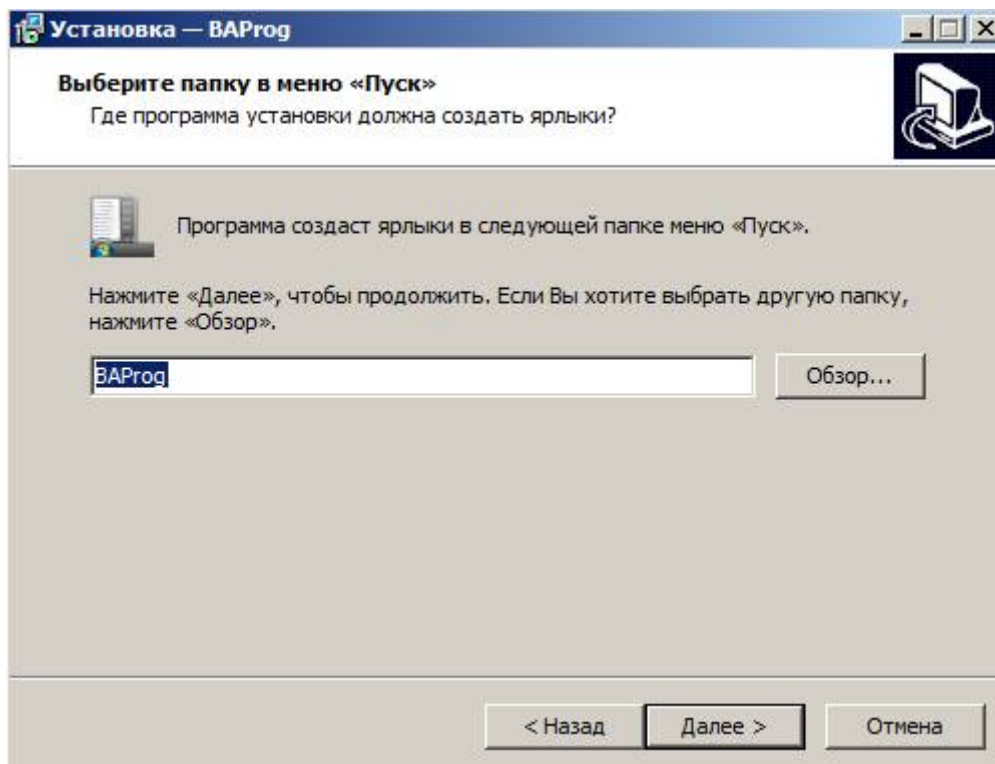


Рисунок 12

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

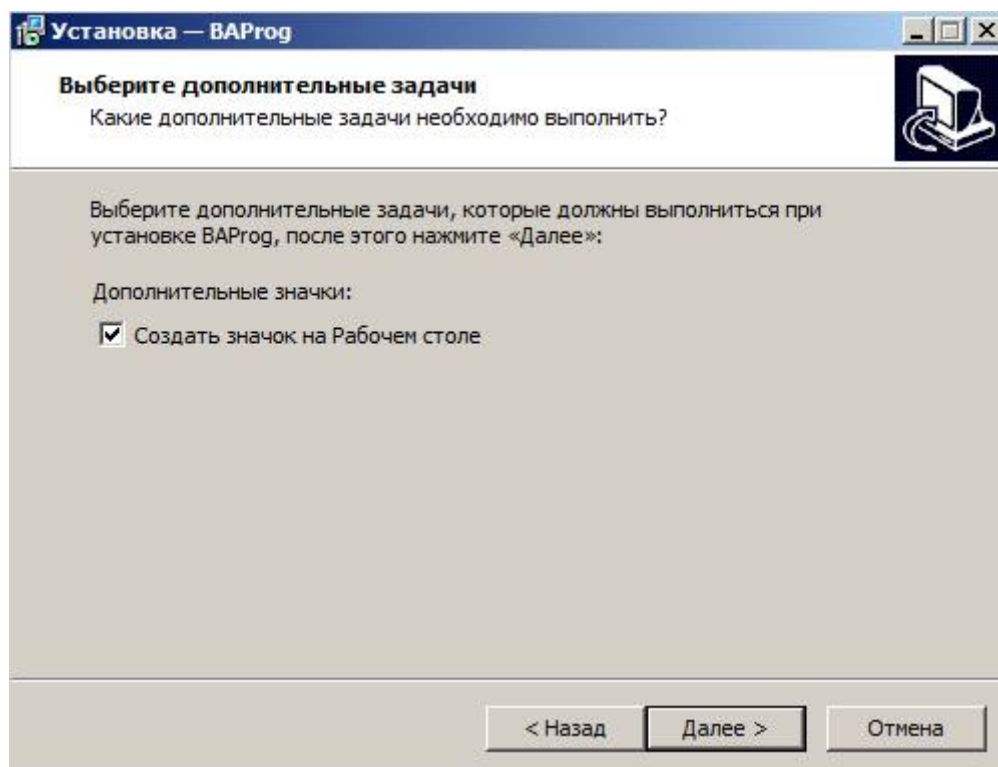


Рисунок 13

C2000-BIOAccess-MA300

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

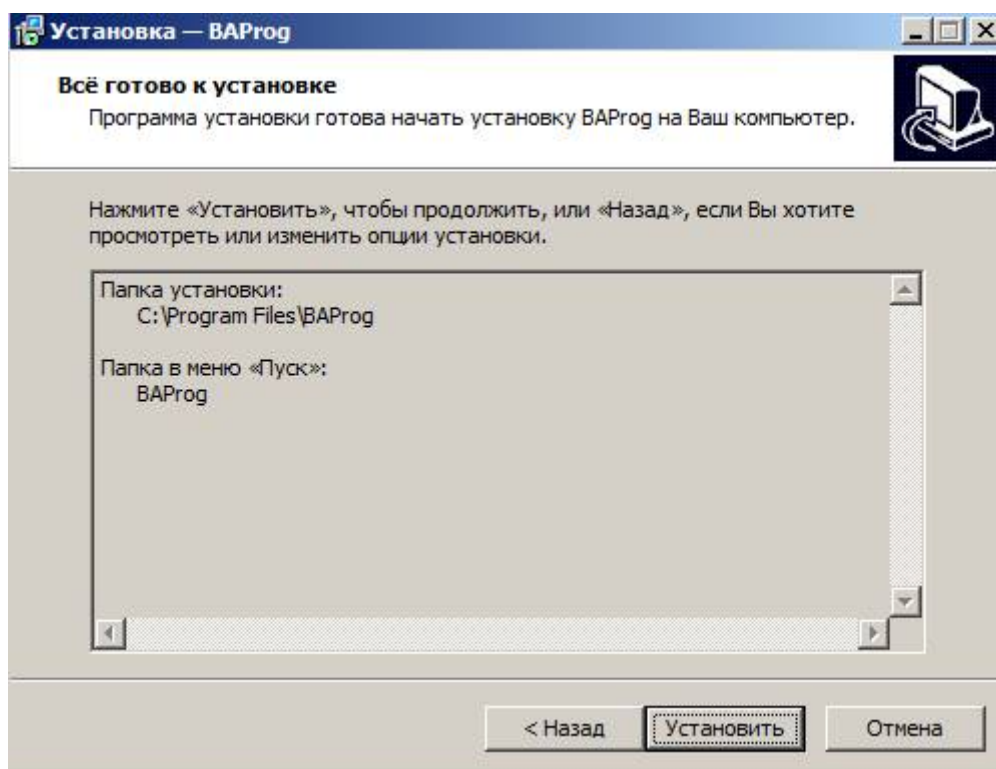


Рисунок 14

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

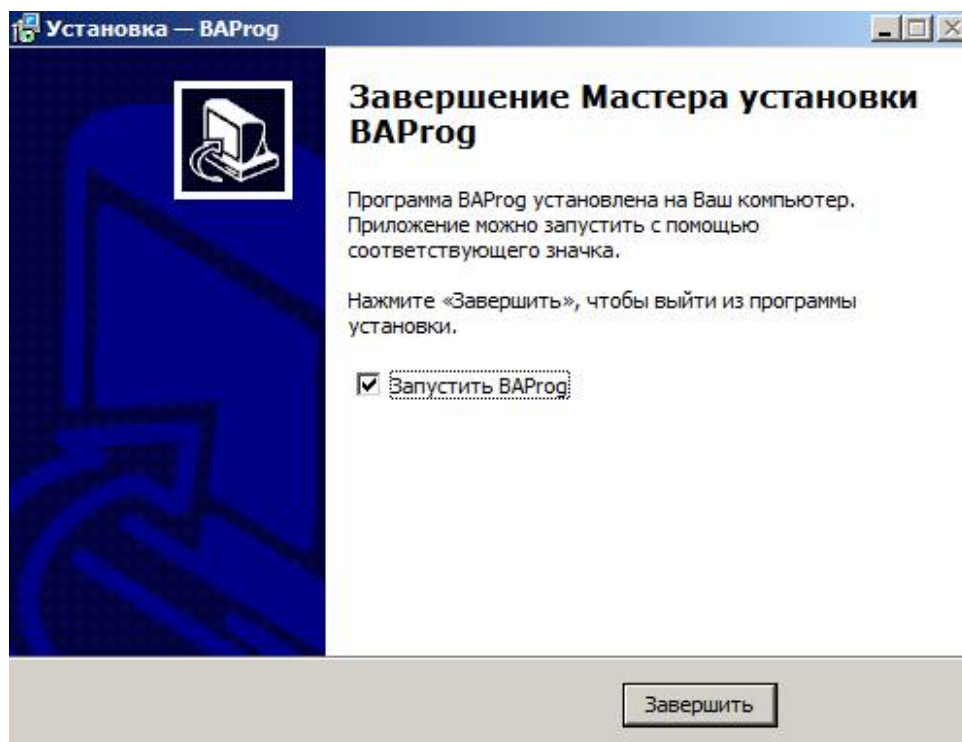


Рисунок 15

Интерфейс ВАProg

При запуске окно ВАProg выглядит следующим образом:

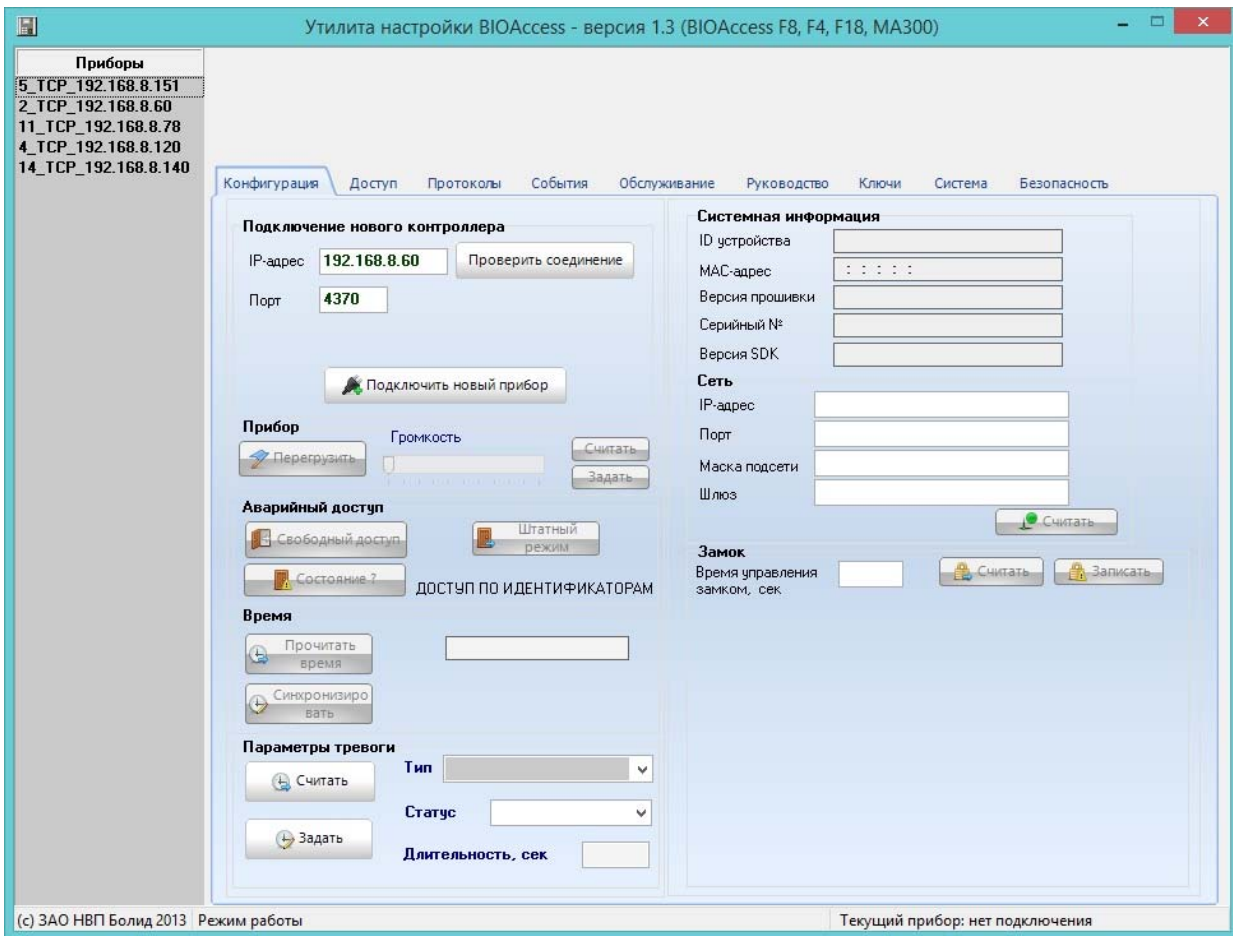


Рисунок 16

В ВАProg рабочие инструменты распределены по следующим вкладкам:

- Конфигурация
- Доступ
- Протоколы
- 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

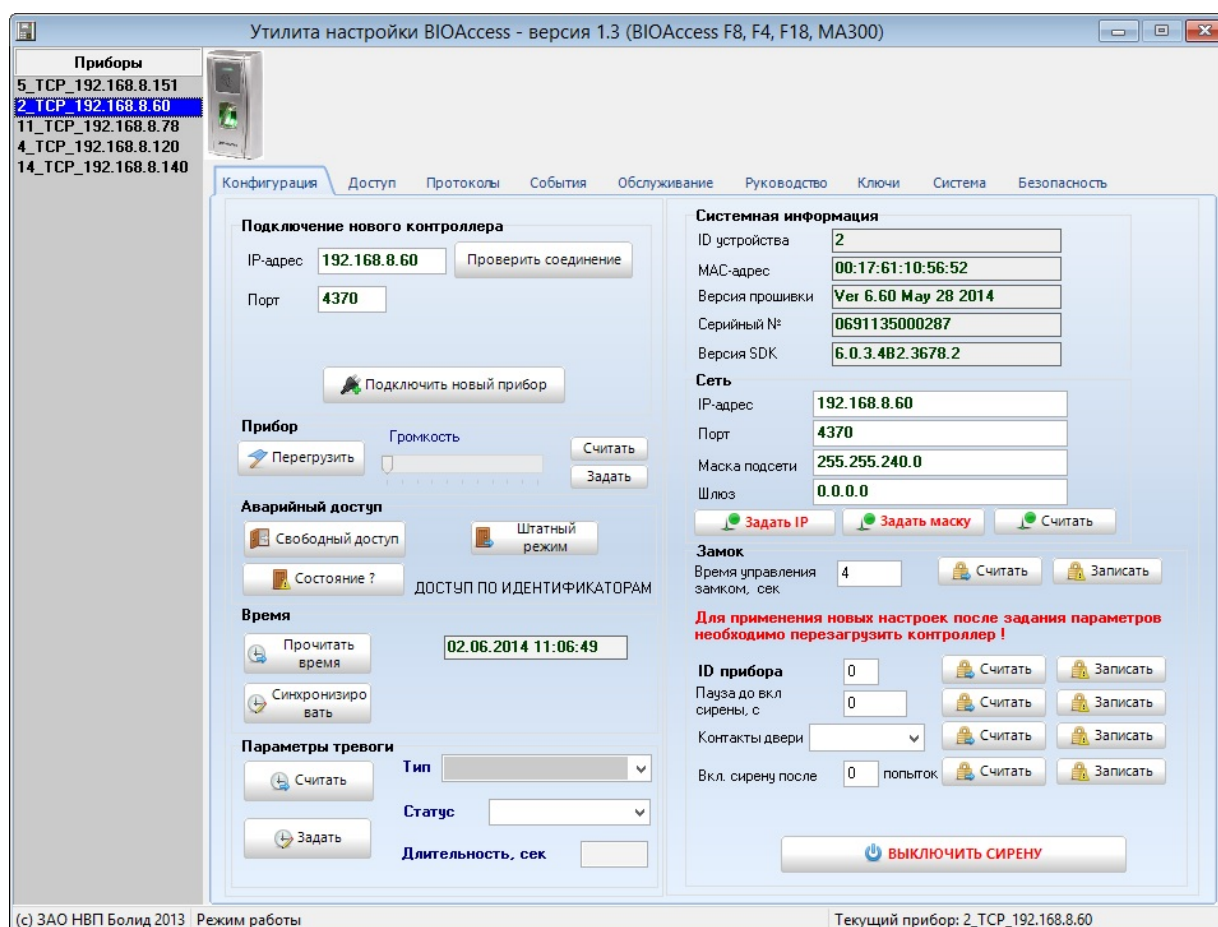


Рисунок 17

В разделе «Подключение нового контроллера» указываются параметры подключаемых приборов - «IP-адрес» и «Порт». Если есть сомнения, 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

При нажатии на кнопку «Подключить новый прибор» программа пытается подключить контроллер с указанными параметрами. Если подключение произошло успешно, то слева в списке подключённых приборов появляется новый контроллер.

Утилита 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 слева.

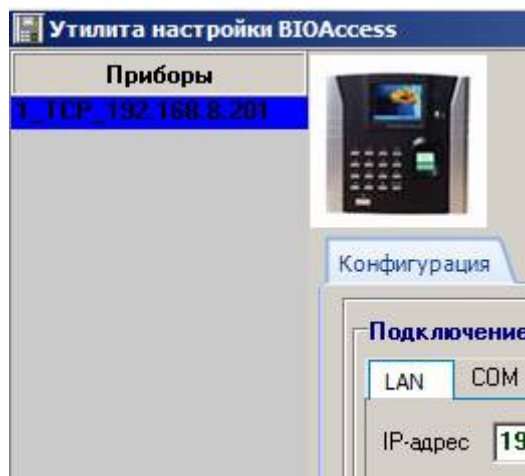


Рисунок 18

Кнопка «Перезагрузить» в поле «Прибор» позволяет при необходимости перезагрузить операционную систему контроллера. Кнопки «Считать/Задать» и ползунок в этом же разделе позволяют считать текущий уровень громкости динамика контроллера, указать его в % перемещением ползунка, и записать этот уровень громкости в прибор, соответственно.

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»).

Кнопка «Считать», расположенная в разделах «Системная информация» и «Сеть» позволяют принудительно вычитать из прибора и отобразить 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. 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. После проведения необходимых настроек можно вернуть «штатное» подключение к корпоративной сети.

В разделе «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». Аналогичным образом можно контролировать и задавать

C2000-BIOAccess-MA300

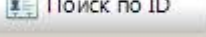
значения для параметров «ID прибора», «Пауза до включения сирены», «Включить сирену после ... попыток» в том же разделе. Кроме того, в выпадающем списке «Контакты двери» можно задать тип подключения контактов замка («Нормально замкнутые» или «Нормально разомкнутые»). Кнопка «Выключить сирену» предназначена для оперативного отключения сирены.

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.

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.

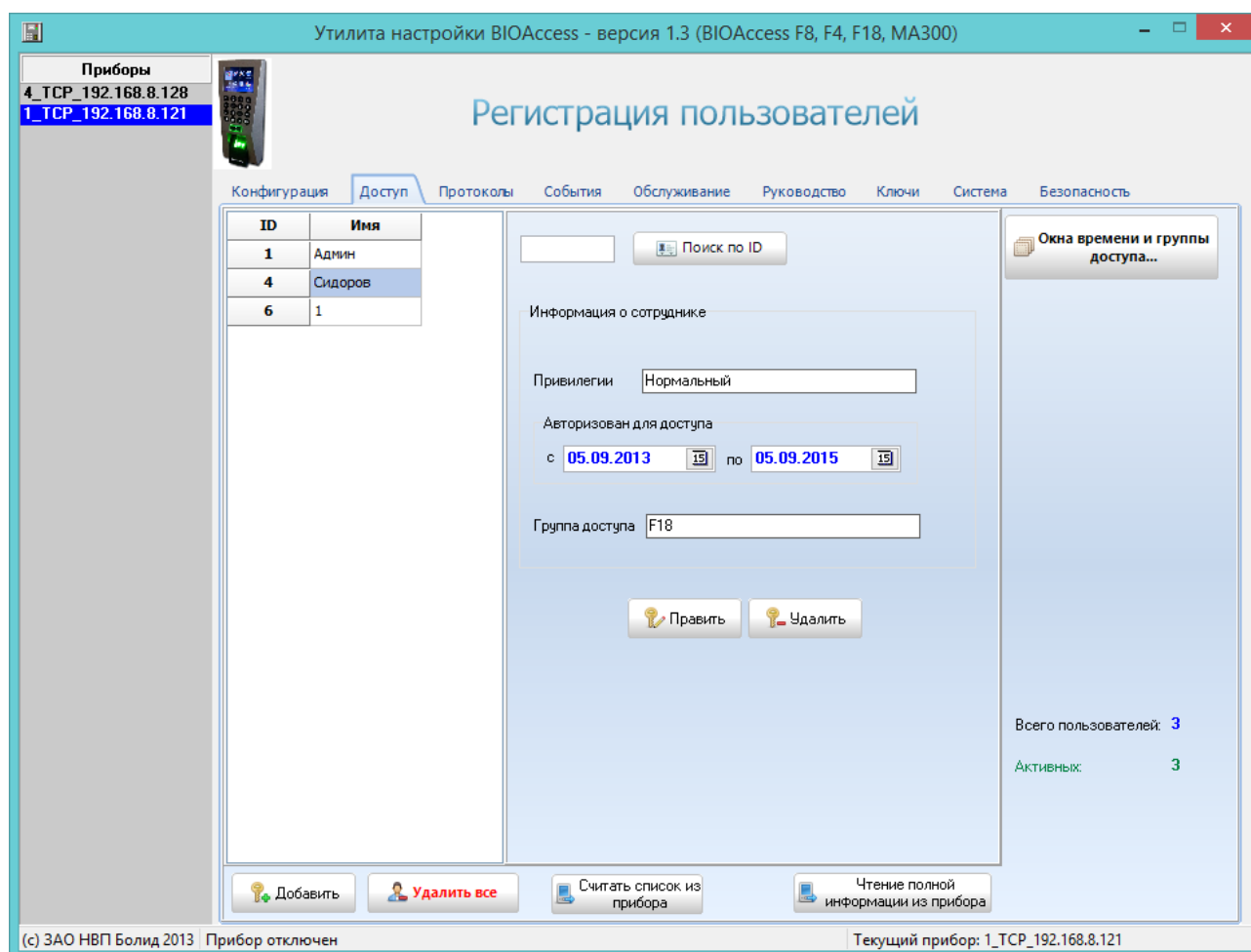
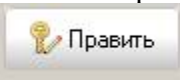


Рисунок 19

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. 26). При нажатии на кнопку «Удалить» появляется запрос на подтверждение операции:

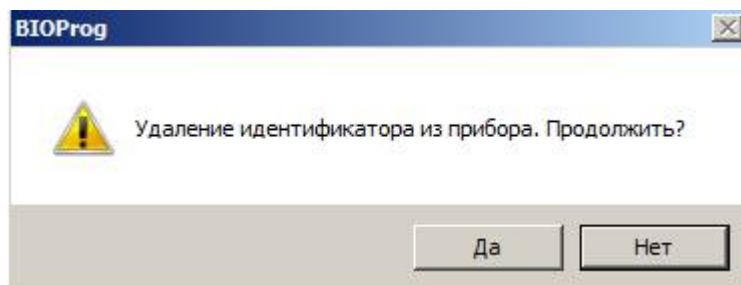
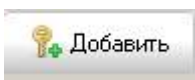

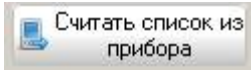
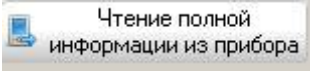
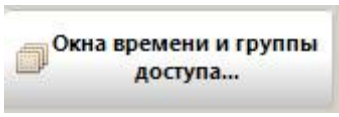


Рисунок 20

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:

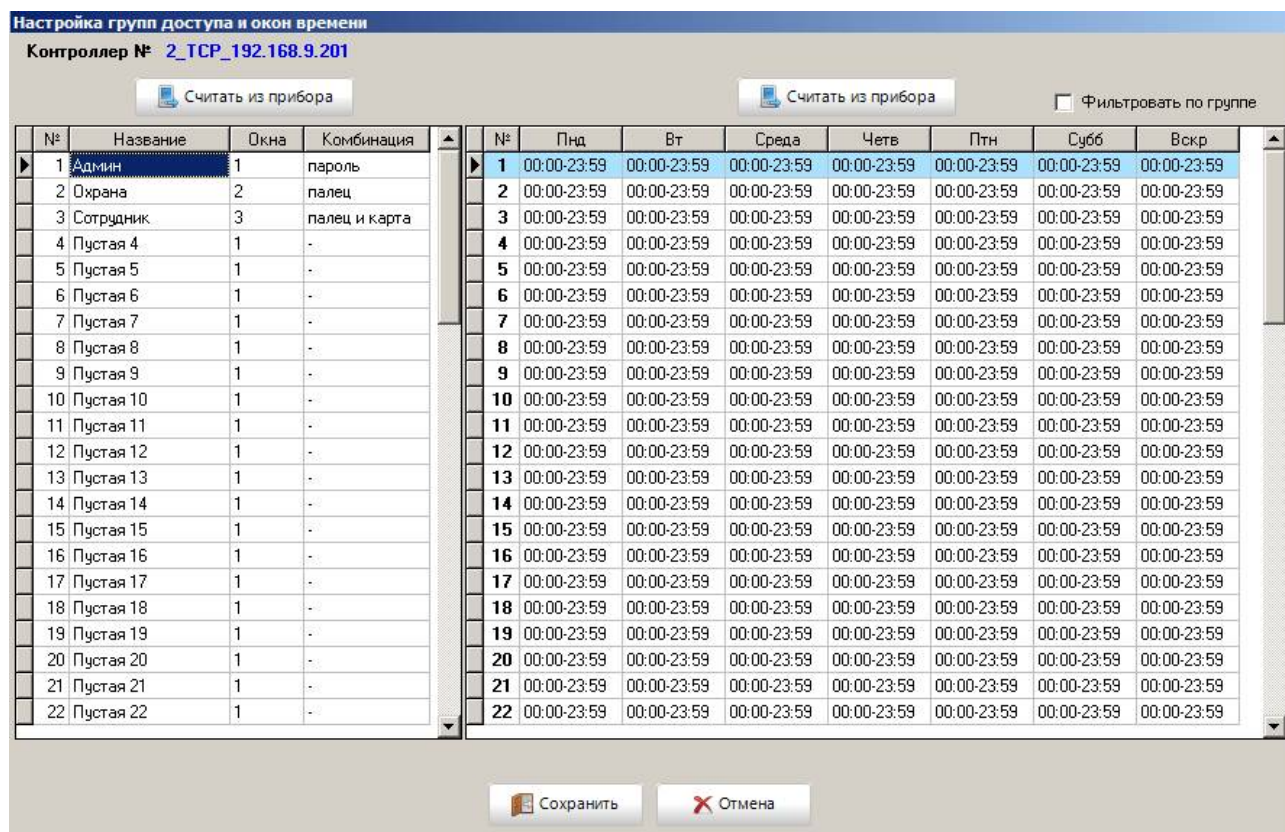
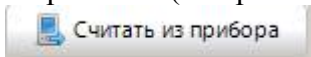


Рисунок 21

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 прочесть 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»:

Номер окна	1	Время входа	Время выхода
Понедельник		00:00	23:59
Вторник		00:00	23:59
Среда		00:00	23:59
Четверг		00:00	23:59
Пятница		00:00	23:59
Суббота		00:00	23:59
Воскресенье		00:00	23:59

Рисунок 22

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»:

Группа доступа

Название:

Окна времени

Окно 1:

Окно 2:

Окно 3:

Комбинация доступа

Отпечаток пальца
 палец + карта

Proximity карта
 палец + пароль

Пароль
 пароль + карта

Рисунок 23

C2000-BIOAccess-MA300

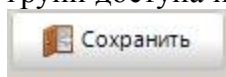
В этом окне можно указать «Название группы». В поле «Окна времени» выбираются необходимые для группы доступа окна времени. С помощью выпадающих списков «Окно 1», «Окно 2» и «Окно 3» можно выбрать до трёх окон времени.

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

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

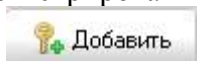
В показанном на рисунке случае выбраны способы аутентификации «Proximity карта» и «Пароль». Это означает, что пользователь может получить доступ при предъявлении карты и пароля.

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

Добавление нового пользователя

ID: Активный

Имя:

Привилегии:

Авторизован для доступа:
с по

Группа доступа:

Конфигурация доступа

Использовать правила группы

Отпечаток пальца палец + карта

Proximity карта палец + пароль

Пароль пароль + карта

пароль + карта + палец

Код карты:

HEX-код:

Пароль:

```
ocoSgba4I8EINDkngRosuiCBFzu
+GMEOREEegRY6TDUBBp3MOYESoExGQQufzELBDZ/QR4ERoCUiARgDMVHBBKAmDAENILQIQVpUKjPBDpCwKQEd
fZsmgQt1oSMBFm0ZGQJEBXjxQoPFMDDAaHd7RjAwnKi/t/rHcDBaG8Bov/+usB+XmFrAQoSgqHaqMB
+XGBqAw4YoeYZI8B+w15pBRMdodqJMB+vilkBhYfodmYJcB+UFFXARqi7ZmJKMB+S0tNOyQim4mJLMB
+SEdFNyuiOYYL8B+SEU+Mql1aHgowH5LRzwvoTd3gsDBRzgrJyaDJ8DCNyiiV6I5JsDDKqJVmYrAxDUkS5gn4AAA
```

Длина шаблона: **360**

Рисунок 24

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 VARprog можно предоставить пользователю привилегии 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 на кнопку . В полях «Код карты» и «HEX-код» появятся считанные значения.

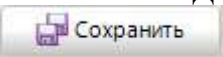
Для регистрации пароля нужный пароль нужно ввести в поле «Пароль».

Для сканирования отпечатка пальца нужно нажать на кнопку
При этом появляется сообщение:



Рисунок 25

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 на кнопку 

Вкладка «Протоколы»

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

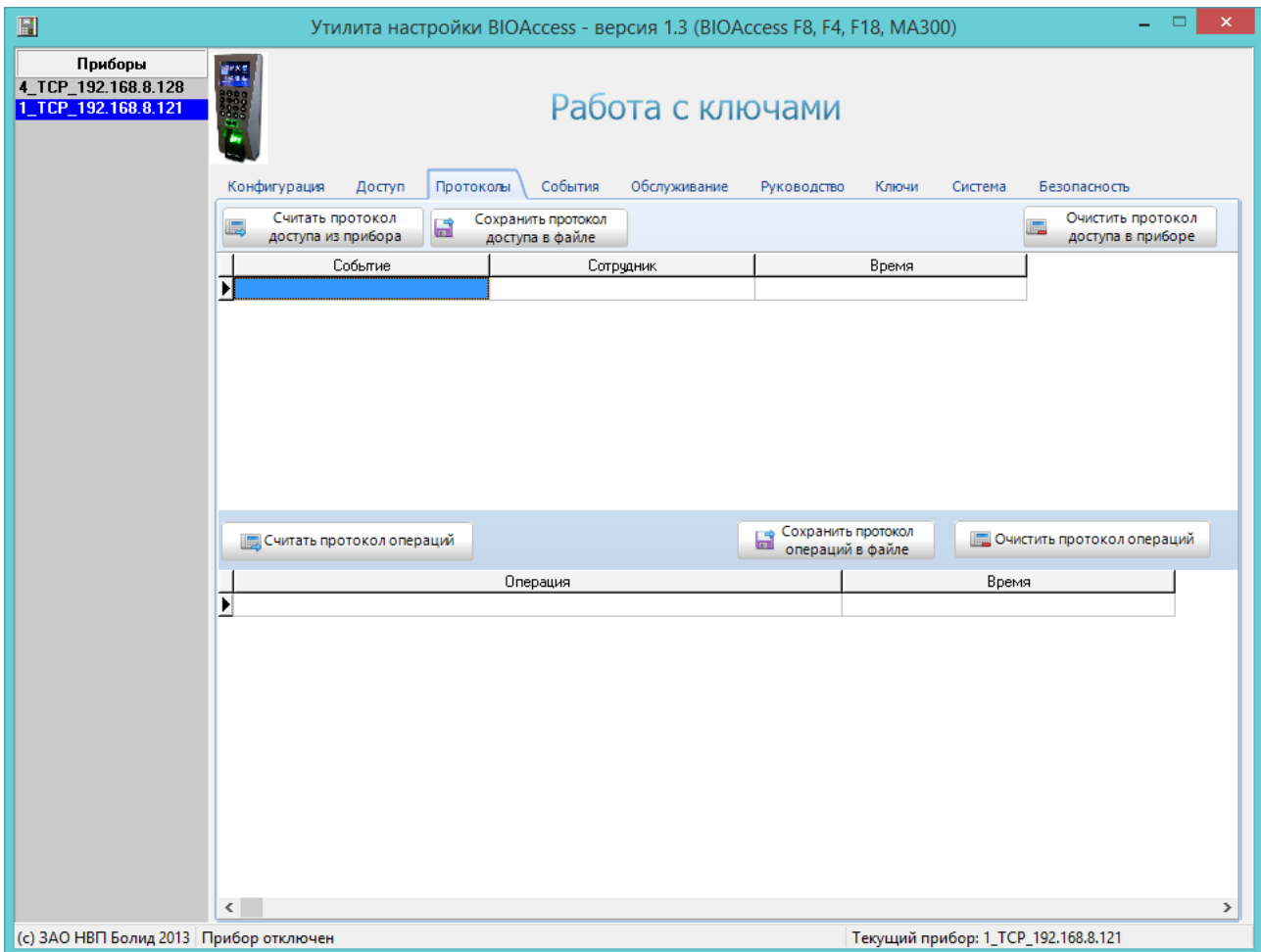
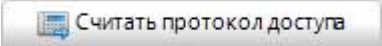
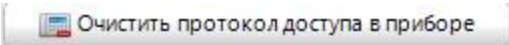
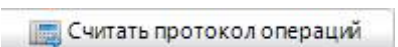
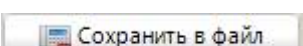
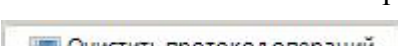


Рисунок 26

На этой вкладке расположены следующие кнопки:

-  – чтение из контроллера журнала доступа;
-  – 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:

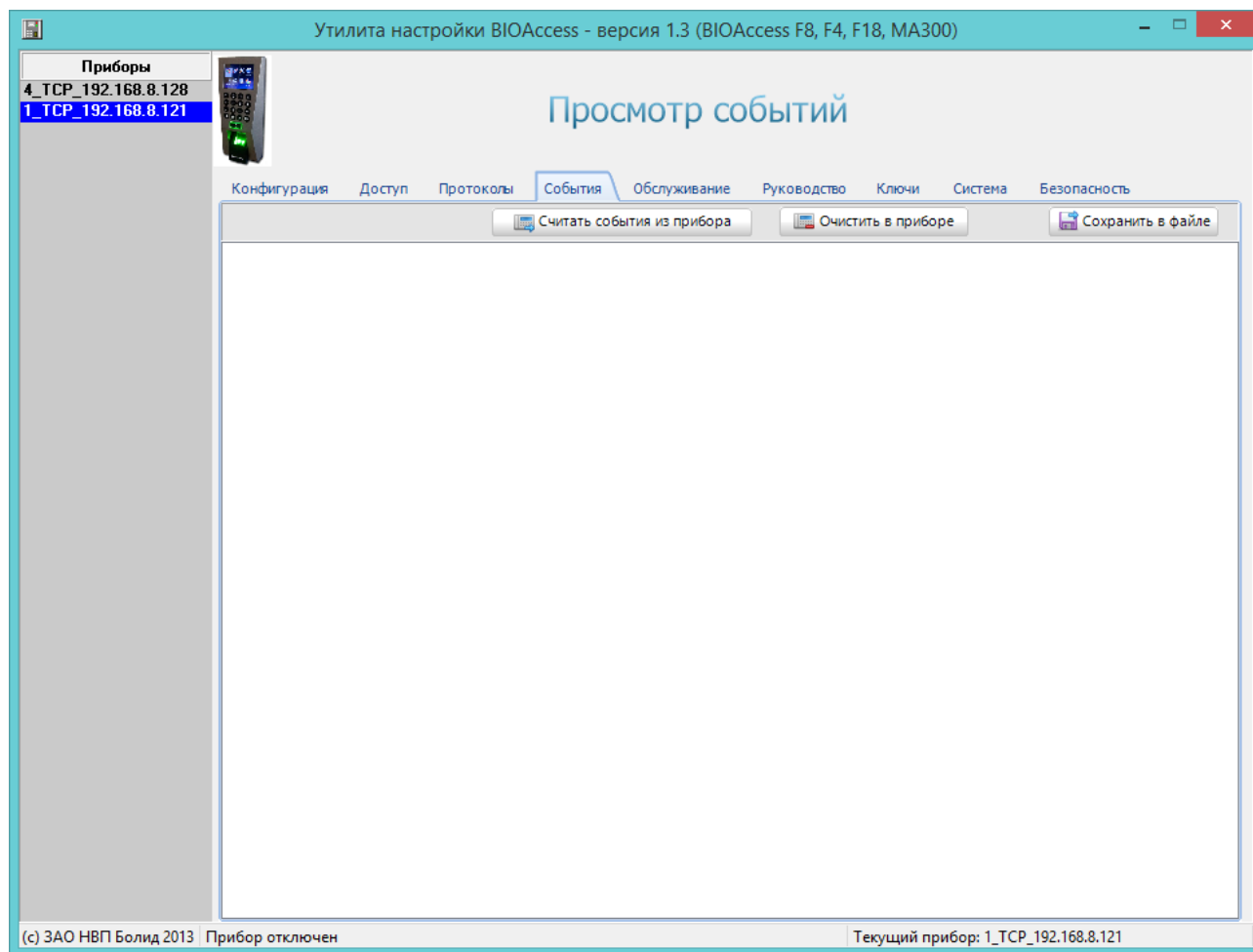
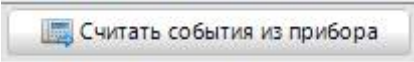
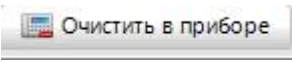



Рисунок 27

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.

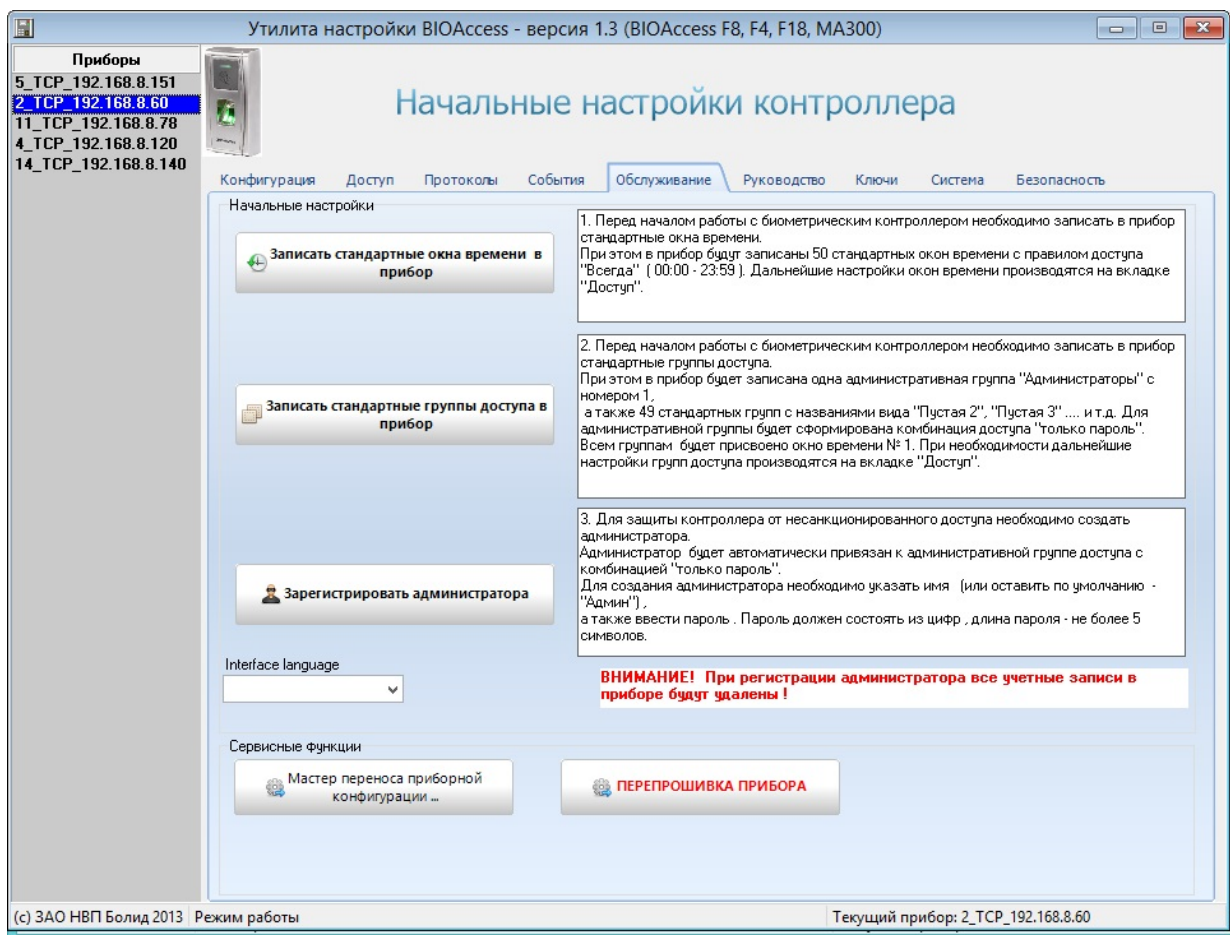
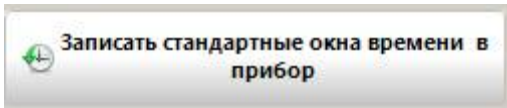
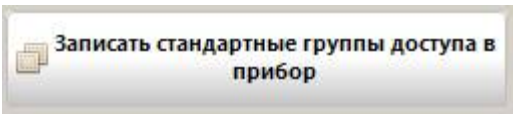
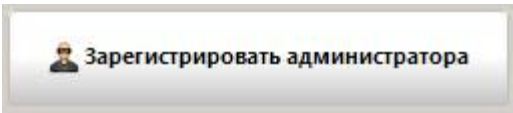
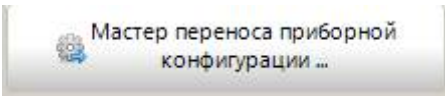


Рисунок 28

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:

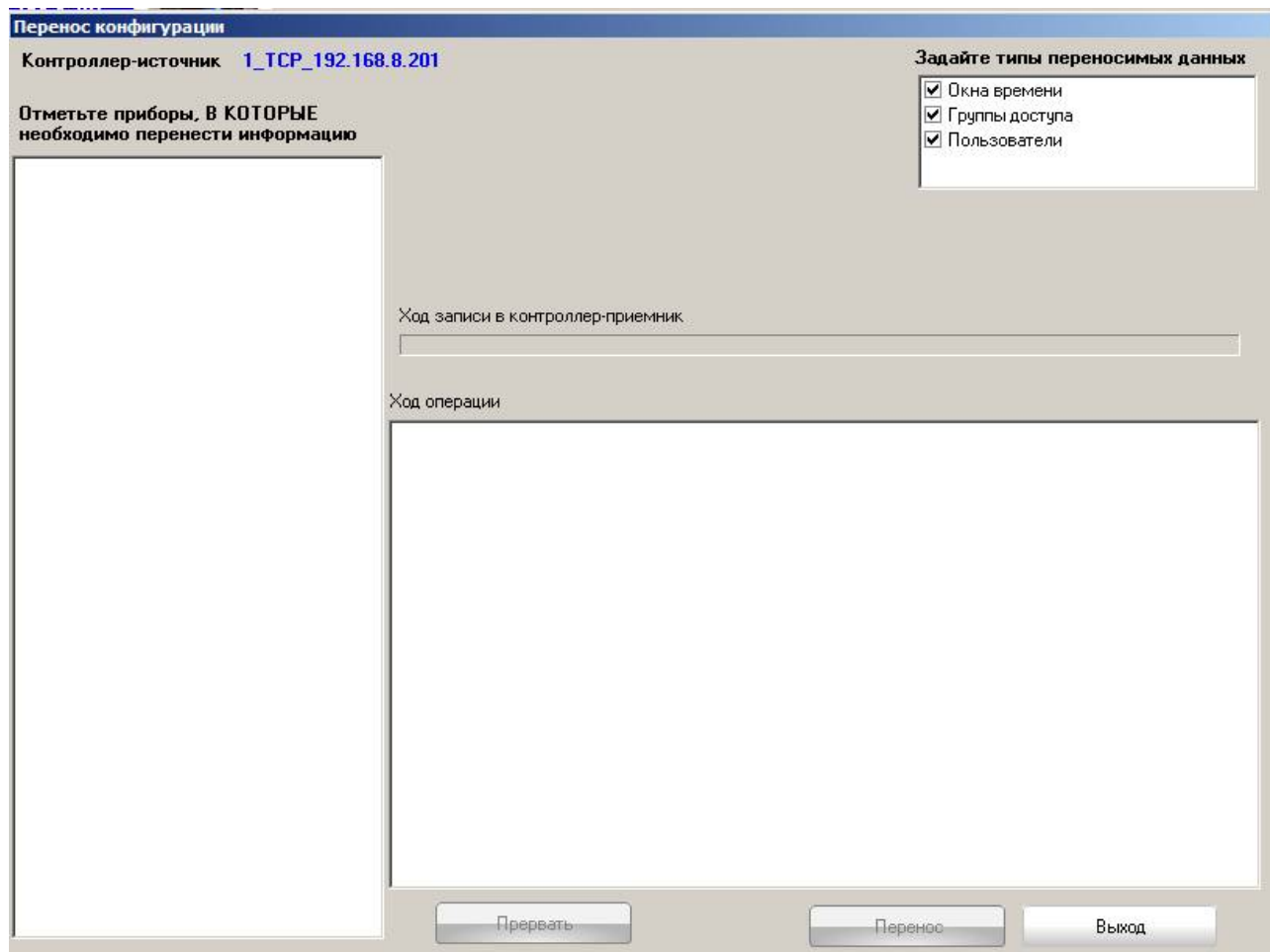


Рисунок 29

В этом окне в строке «Контроллер-источник» показано название контроллера, который выбран в VARprog 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».

Кнопка «Перепрошивка» используется для обновления встроенного программного обеспечения биометрического контроллера. Категорически не рекомендуется пользоваться данной кнопкой без явного указания технической поддержки или технического консультанта компании «Болид».

Вкладка «Руководство»

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

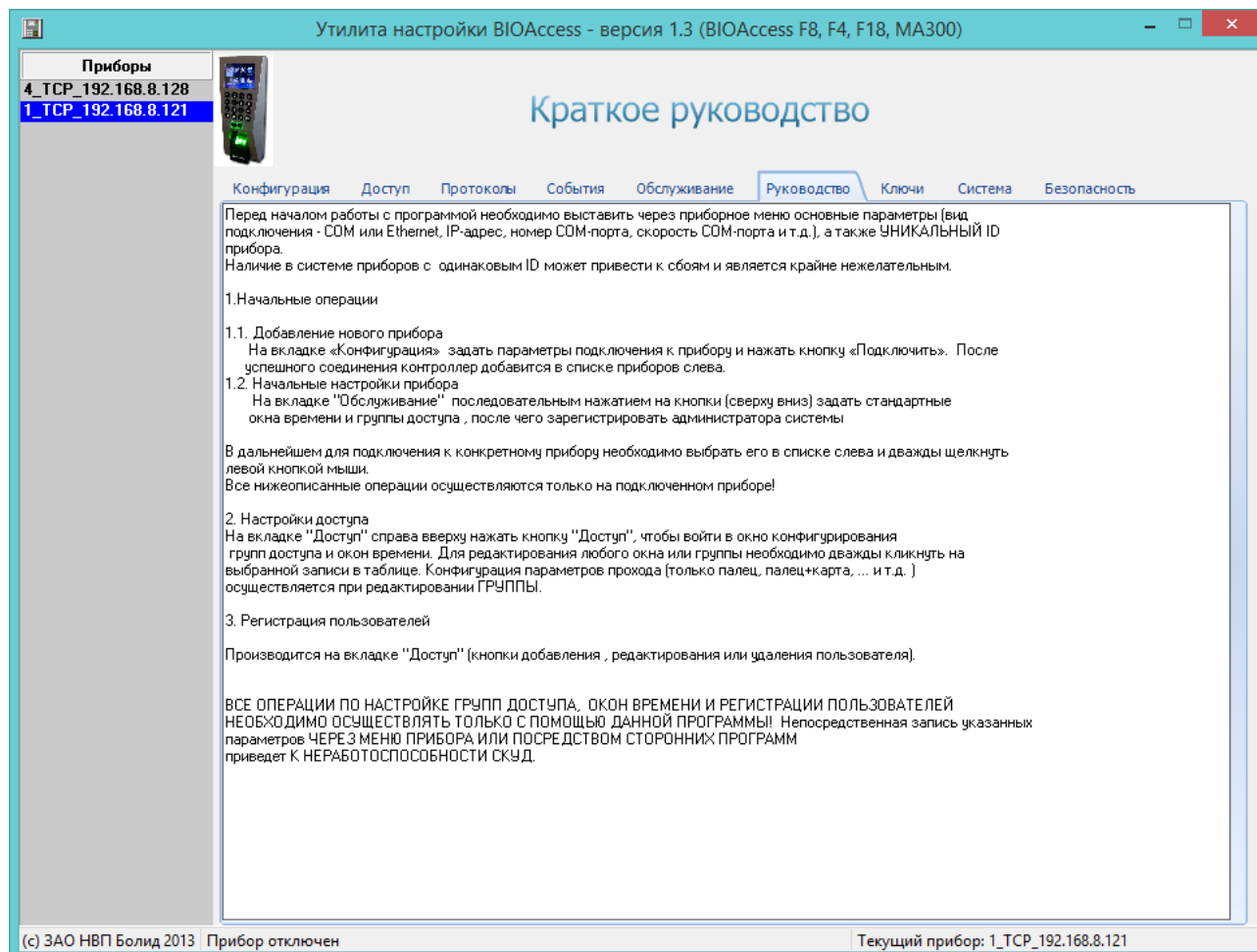


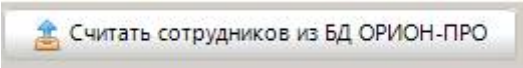

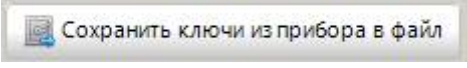
Рисунок 30

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:

-  Считать сотрудников из БД ОРИОН-ПРО – загрузить список сотрудников из базы данных «Орион Про».
-  Записать ключи из файла в прибор – загрузить информацию о пользователях из файла в контроллер.
-  Сохранить ключи из прибора в файл – сохранить информацию о пользователях, записанную в контроллере, в файл.

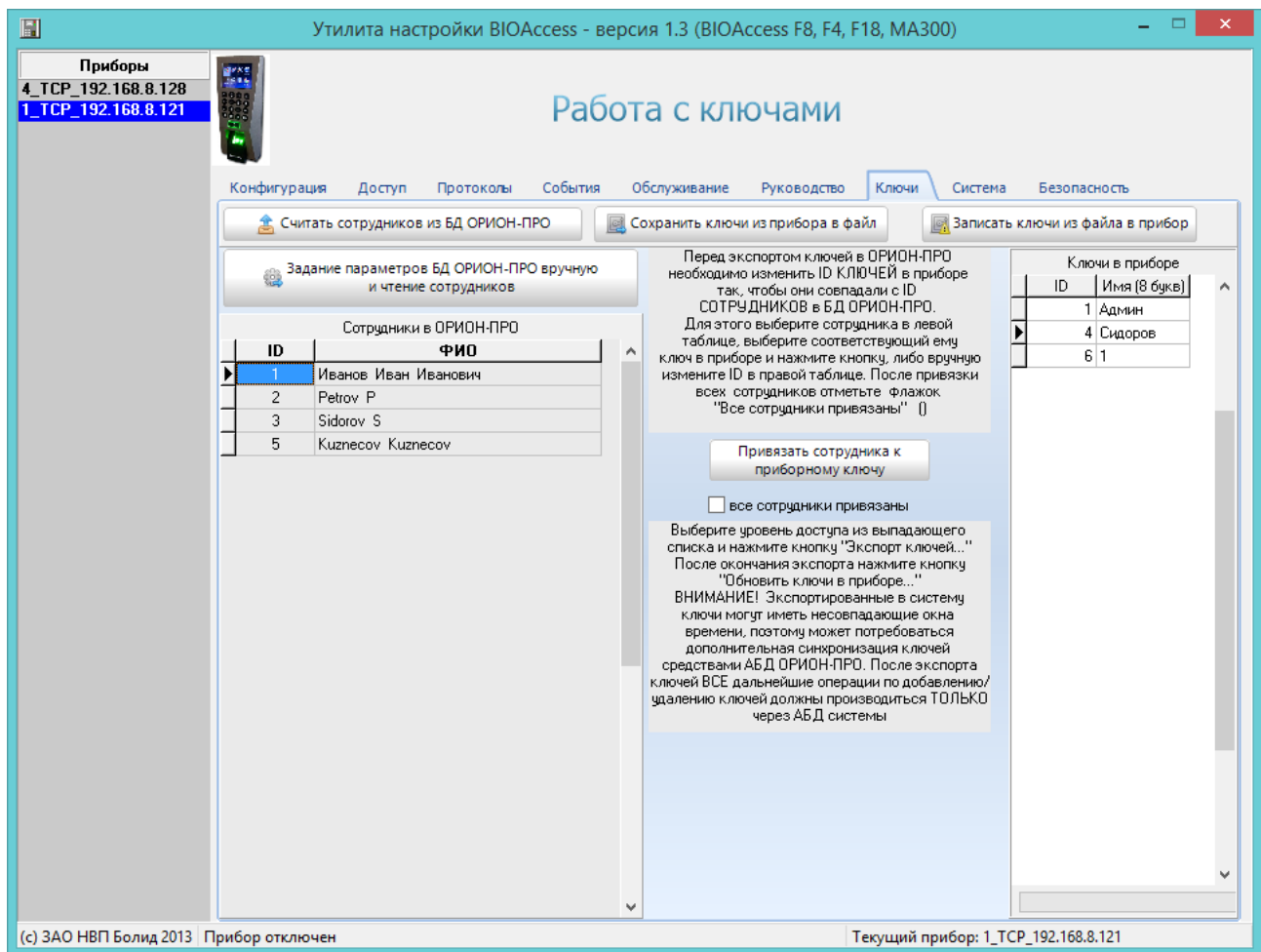
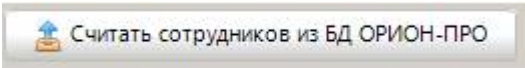
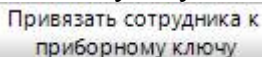


Рисунок 31

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

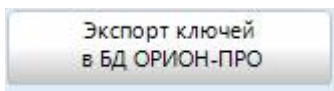
В левом столбце после нажатия на кнопку  показывается список сотрудников, зарегистрированных в базе данных «Орион Про».

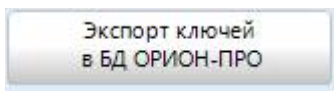
Перед экспортом ключей в «Орион Про» необходимо изменить номера (ID) ключей в контроллере так, чтобы они совпадали с ID сотрудников в базе данных «Орион Про». Для этого нужно выбрать сотрудника в списке «Сотрудники в ОРИОН-ПРО», выбрать соответствующую ему запись в списке «Ключи в приборе» и нажать на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

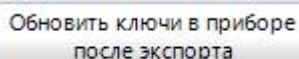


. Также можно назначить нужный номер, выполнив двойной щелчок левой кнопкой мыши на изменяемом номере.

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».

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»

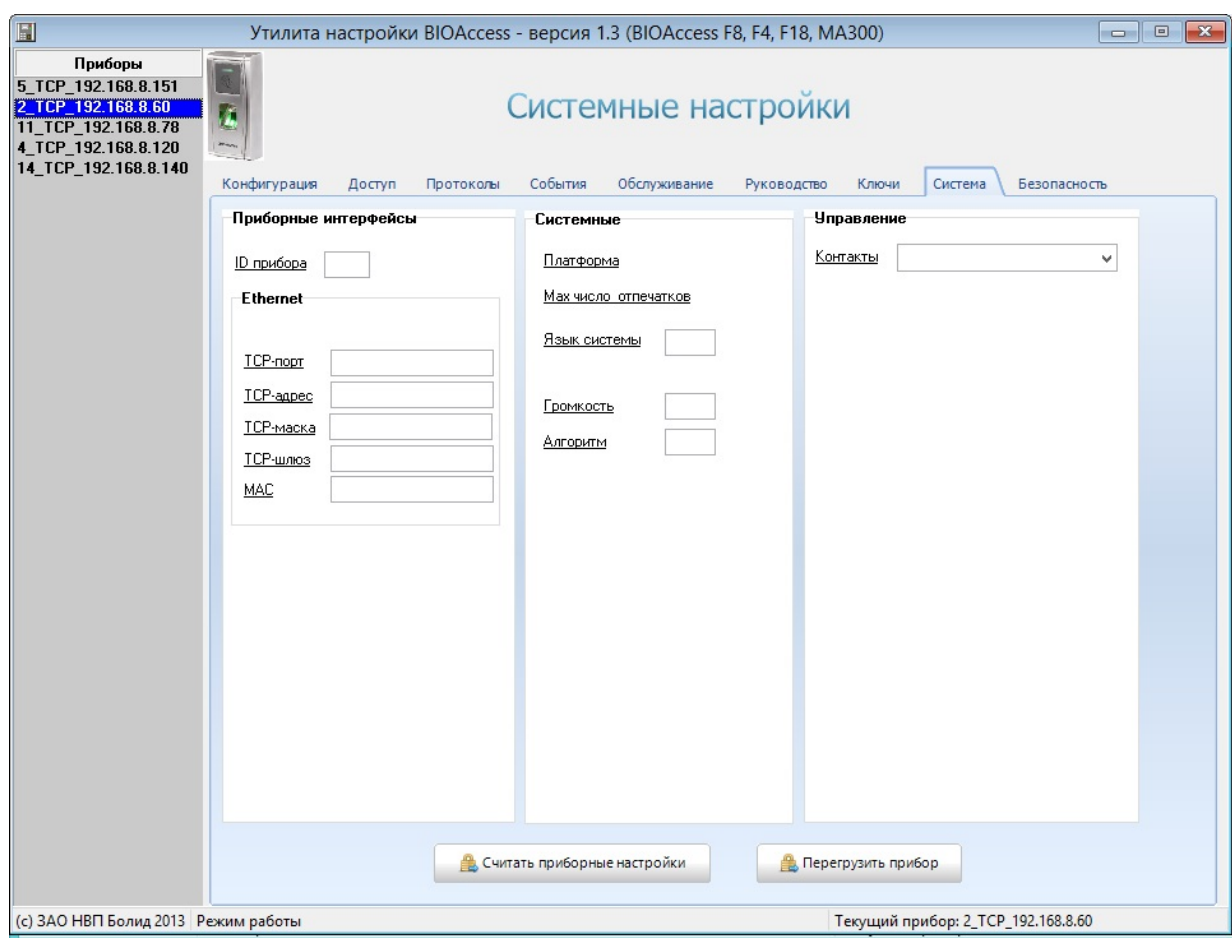


Рисунок 32

Вкладка «Безопасность»

Данная вкладка предназначена для задания параметров защищенного режима (ЗР). Этот режим реализован только в контроллерах C2000-BIOAccess -MA-300 и -F18.

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

В этом режиме электрозамок двери управляется от контроллера типа C2000-2, к которому в качестве Wiegand-считывателя подключается биометрический контроллер.

Для реализации ЗР необходимо:

1. В биометрическом контроллере задать ID и код проксимити-карты ("секретной" карты)
2. Включить режим ЗР
3. В контроллере семейства C2000-2 зарегистрировать пользователя с данным ключом доступа (код ЭТОЙ ЖЕ "секретной" карты), и дать ему полномочия на проход.

ВАЖНО! В биометрическом контроллере и в контроллере C2000-2 должен быть зарегистрирован только ОДИН ключ доступа - это код "секретной карты".

Не нужно регистрировать/дублировать в C2000-2 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.)

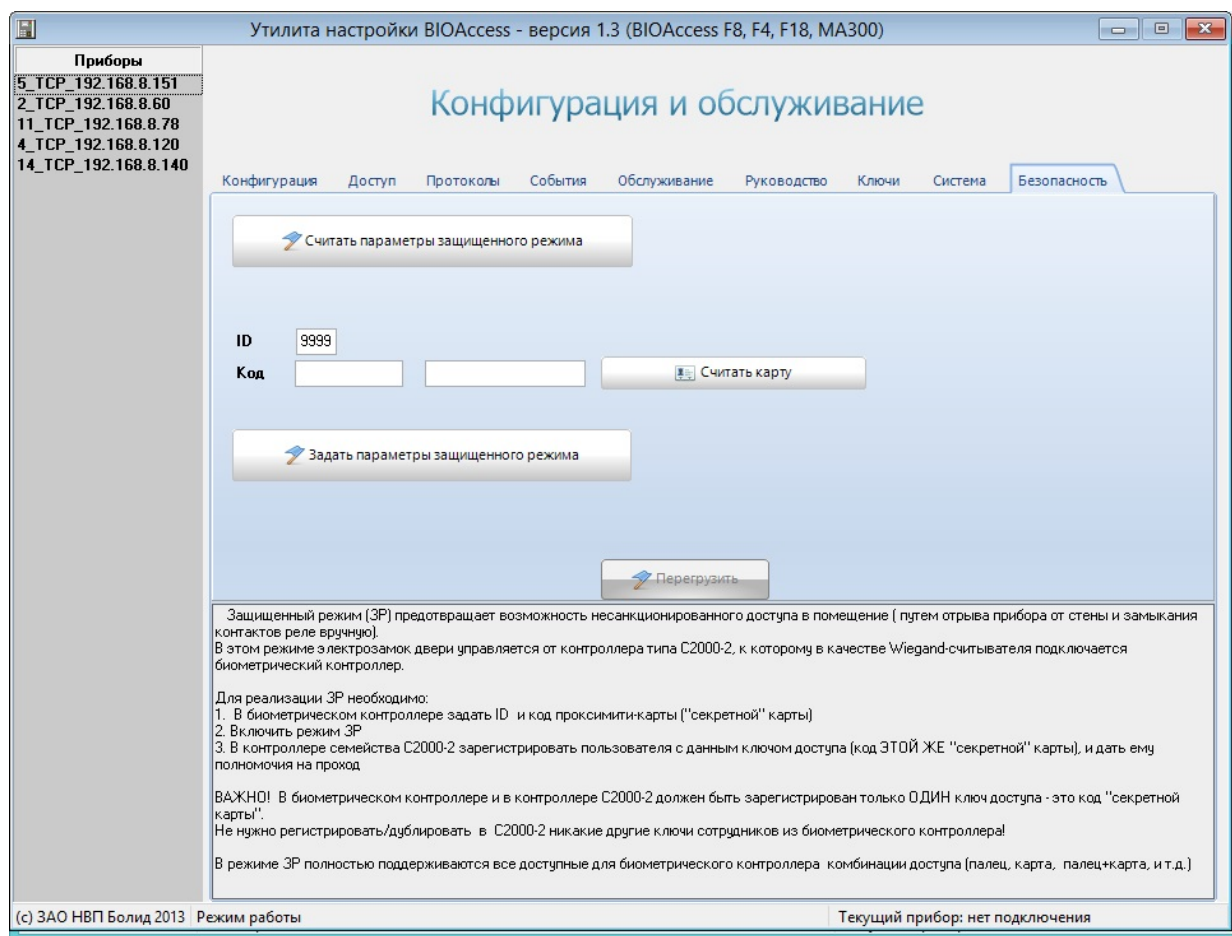


Рисунок 33

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 ко входам Wiegand D1-1 и D0-1 контроллера С2000-2 соответственно. Таким образом, в данном режиме биометрический контроллер МА300 используется контроллером С2000-2 в качестве считывателя проксимити-карт.

Для включения режима необходимо в поле «Код» ввести код проксимити-карты («секретной карты»). Это может быть сделано вручную, либо путем считывания кода 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 проксимити-карты.

Принцип работы режима ЗР следующий. После успешной верификации отпечатка пальца (или любой комбинации типа только карта, палец+карта) биометрический контроллер выдает 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.

В качестве управляющего дверью контроллера может использоваться не только С2000-2, но и любой другой контроллер, поддерживающий Wiegand-считыватели проксимити-карт.

Начальная настройка контроллера

Настройка сетевых параметров

Специфической особенностью данного контроллера является отсутствие клавиатуры и дисплея. Вследствие этого, сетевые параметры подключения могут быть заданы только с использованием программного обеспечения (утилиты ВАРog).

На вкладке «Конфигурация и обслуживание» имеются специальные кнопки «Задать IP» и «Задать маску» для изменения IP-адреса и маски подсети соответственно. Перед изменением адреса или маски необходимо ввести новые значения в поля ввода, как показано на рис.

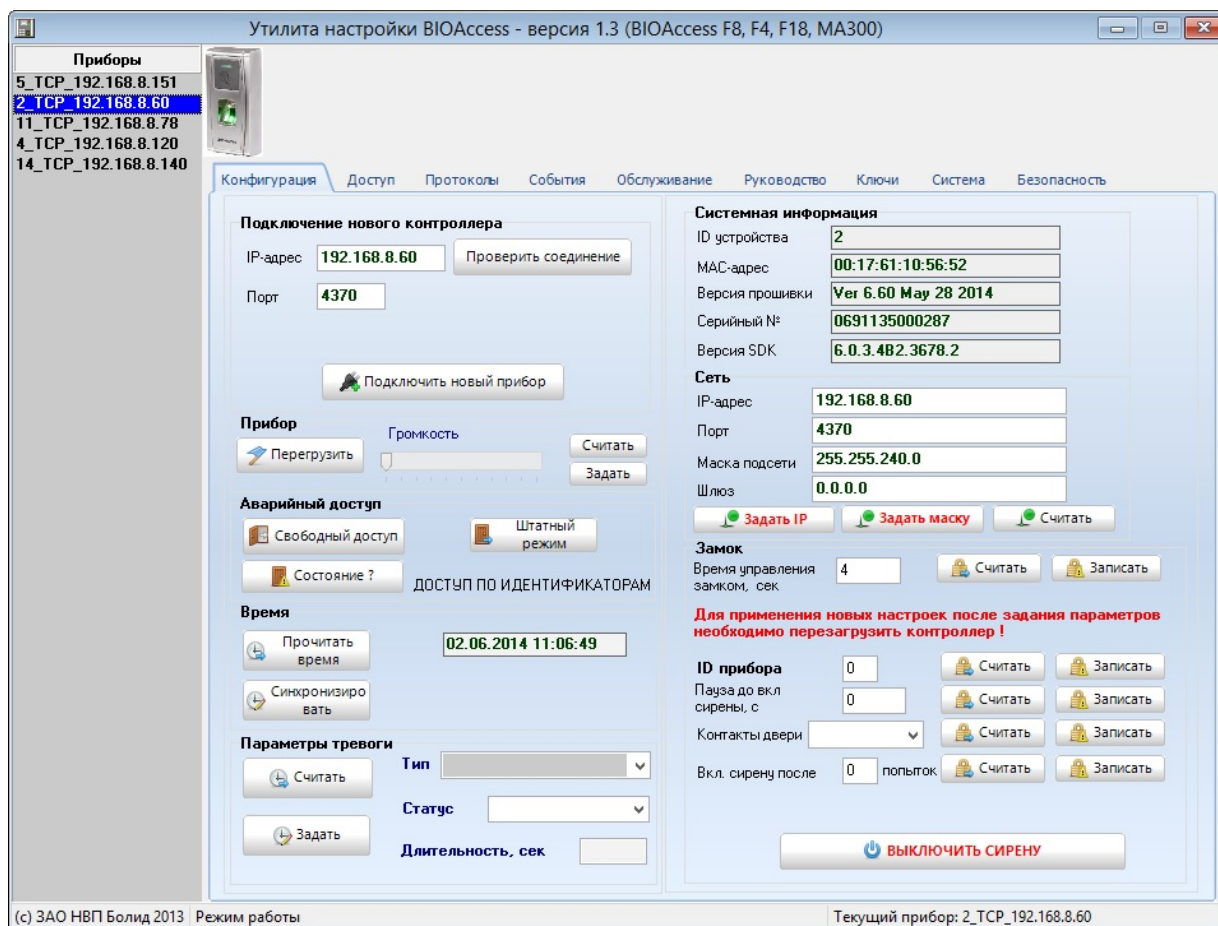
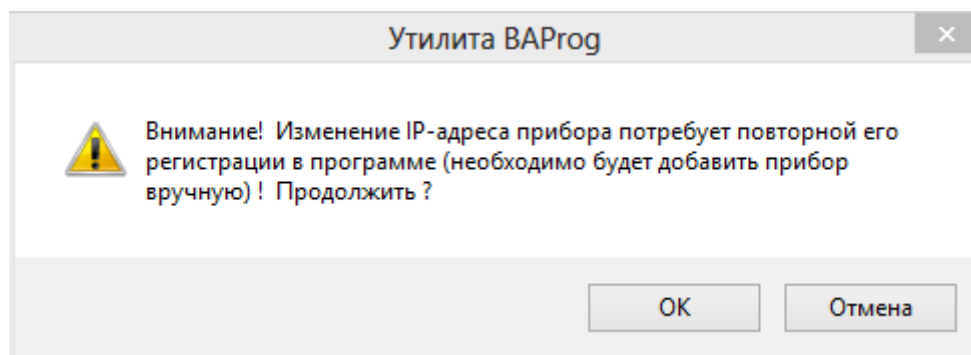


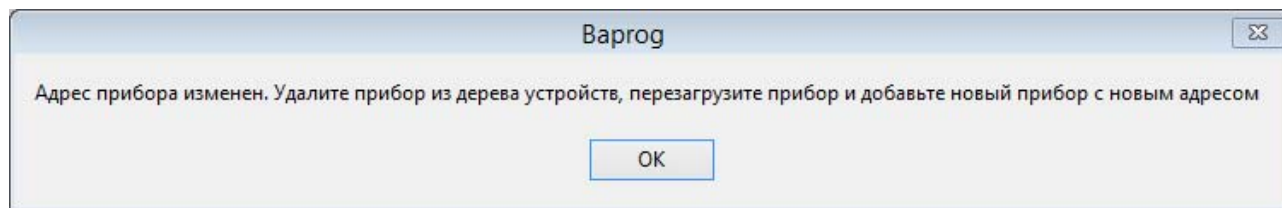
Рисунок 34

Важно! Каждый параметр (адрес или маска) может быть изменен только отдельно! То есть для смены и адреса и маски потребуются две отдельные операции.

После задания IP-адреса в поле ввода необходимо нажать кнопку «Задать IP». При этом на экране появится окно с предупреждением:



После нажатия кнопки «ОК» начнется процедура смены IP-адреса в устройстве, после завершения которой появится окно с сообщением:



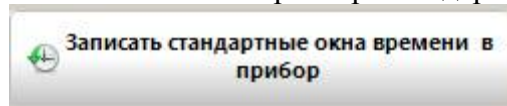
Далее необходимо нажать кнопку «ОК» и проделать указанные в данном сообщении операции.

Установка сетевой маски осуществляется аналогично.

Настройка параметров доступа

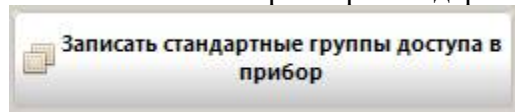
Для того чтобы контроллер можно было использовать в ИСО «Орион Про», необходимо на вкладке «Обслуживание» программы VARprog выполнить следующие операции:

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



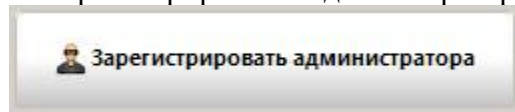
, в появившемся окне подтвердить выполнение операции (нажать на кнопку «ОК»). При этом в контроллер будут записаны 50 стандартных окон времени с правилом доступа «Всегда» (00:00-23:59).

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.

Настройка контроллера в VARprog

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

1. Выполнение начальной настройки контроллера.
2. Программирование окон времени.
3. Настройка групп доступа.
4. Регистрация пользователей.
5. Редактирование времени управления замком.

Обслуживание контроллера через VARprog сводится к следующим действиям:

1. Редактирование окон времени.
2. Редактирование групп доступа.
3. Добавление/удаление/редактирование пользователей.
4. Предоставление аварийного доступа.
5. Перезагрузка контроллера.
6. Копирование базы данных контроллера в другие приборы.
7. Синхронизация времени.

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.

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. **В акте также необходимо указывать сетевые настройки 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>

Сведения о сертификации

Биометрический контроллер доступа «С2000-БИОAccess-МА300» соответствует требованиям технического регламента Таможенного союза ТР ТС 020/2011. Имеет сертификат соответствия № RU С-RU.ME61.B.00445