ИСО «Орион»

Биометрический контроллер доступа

C2000-BIOAccess-F18

Руководство пользователя

Настоящее руководство пользователя предназначено для изучения принципов работы и эксплуатации биометрического контроллера доступа «С2000-BIOAccess-F18».

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 (номер, пароль, Proximity-карта, отпечаток пальца).

Содержание

Общие сведения

Биометрический контроллер доступа «С2000-BIOAccess-F18» (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, встроенным считывателем Proximity-карт и клавиатурой для ввода пароля.

Контроллер обеспечивает световую, текстовую, графическую 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 любых идентификаторов (отпечаток пальца, Proximity-карточка, пароль).

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 и отображает их на своём дисплее.

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

Настройка контроллера «С2000-BIOAccess-F18» выполняется с помощью программы конфигурирования биометрических контроллеров BAProg. Новейшую версию программы BAProg 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, защищённых от воздействия атмосферных осадков и ударных воздействий, и рассчитан на непрерывную круглосуточную работу. Конструкция контроллера не предусматривает его использование в условиях воздействия агрессивных сред, пыли, 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.

ВНИМАНИЕ! Во избежание несанкционированного доступа необходимо зарегистрировать в контроллере пользователя с правами администратора с доступом по отпечатку пальца или паролю. В противном случае в меню контроллера можно будет зайти любому человеку без пароля и отпечатка.

ПРИ РАБОТЕ В СКУД ВСЕ ОПЕРАЦИИ ПО НАСТРОЙКЕ ГРУПП ДОСТУПА, ОКОН ВРЕМЕНИ И РЕГИСТРАЦИИ ПОЛЬЗОВАТЕЛЕЙ НЕОБХОДИМО ОСУЩЕСТВЛЯТЬ ТОЛЬКО С ПОМОЩЬЮ ПРОГРАММЫ BAPROG! Непосредственная запись указанных параметров ЧЕРЕЗ МЕНЮ КОНТРОЛЛЕРА ИЛИ 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 0 до 45 ºС. 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 цифровые пароли или 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:

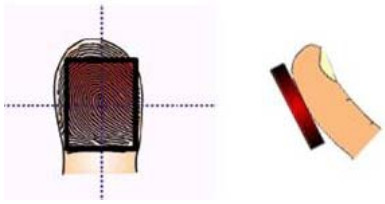


Рисунок 1. Правильное положение пальца при сканировании

Методы верификации отпечатков пальцев

Контроллер поддерживает два метода верификации отпечатков пальцев: 1:1 и 1:N.

При методе верификации 1:N отсканированный отпечаток пальца сравнивается со всеми шаблонами в базе данных контроллера.

При методе верификации 1:1 пользователю необходимо перед сканированием отпечатка пальца указывать свой номер (ID), набрав его на клавиатуре контроллера. В этом случае отсканированный отпечаток пальца сравнивается только с шаблоном пользователя с указанным номером.

В случае использования аутентификации по Proximity-карте и отпечатку пальца верификация отпечатка тоже может осуществляться по методу 1:1. Для этого пользователю нужно сначала приложить к считывателю Proximity-карту, а затем отсканировать отпечаток пальца.

Уровни порога соответствия

Уровни порога соответствия устанавливают баланс между вероятностью ложного принятия (FAR) отпечатка пальца и вероятностью ложного отклонения (FRR) отпечатка пальца. Величина FAR обозначает вероятность предоставления доступа пользователю, не имеющему необходимых прав. Величина FRR обозначает вероятность отказа в доступе пользователю, обладающему необходимыми правами.

Рекомендуемые значения настройки порога соответствия для методов верификации приведены в таблице 1.

Таблица 1. Рекомендуемые значения порогов соответствия

FRR	FAR	1:N	1:1
высокая	низкая	45	25
средняя	средняя	35	15
низкая	высокая	25	10

Внешний вид, органы управления

Рисунок 2. Лицевая панель C2000-BIOAccess-F18

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

1) цветной графический TFT ЖК-дисплей диагональю 2.4 дюйма
2) клавиатура и область считывателя Proximity-карт
3) светодиодный индикатор
4) считыватель отпечатков пальцев

Цветной графический TFT ЖК-дисплей диагональю 2.4 дюйма служит для отображения системных сообщений и навигации по меню контроллера.

Клавиатура контроллера состоит из 17 кнопок: «1», «2»,..., «0», «🔔», «M/OK», «C», «▲», «▼», «◄», «►».

Внутри корпуса, по контуру клавиатуры, расположена антенна считывателя Proximity-карт.

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

Таблица 2. 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

С левой стороны контроллера находится кнопка «Reset», позволяющая перезагрузить контроллер. Здесь же находятся разъём для подключения USB-накопителя и громкоговоритель.

На тыльной стороне контроллера находятся разъёмы соединительных проводов и кнопка датчика контроля вскрытия 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	3000
➢ Объём буфера событий, записей	30 000
➢ Диапазон температур, ºС	от 0 до +45
➢ Относительная влажность воздуха, %	от 20 до 80
➢ Габаритные размеры, мм	не более 80×183×42
➢ Масса, кг	не более 0,7

Подготовка к эксплуатации

Перед использованием контроллера нужно удалить защитные плёнки с экрана и считывателя отпечатков пальцев.

Для проверки работоспособности контроллера необходимо выполнить следующую последовательность действий:

1. Подать питание на контроллер.
2. Включается подсветка экрана. На экране появляется заставка загрузки операционной системы. Светодиодный индикатор выключен.
3. В течение 1 мин после включения питания контроллер должен перейти в рабочий режим. При этом на дисплее отображаются текущие дата и время; светодиодный индикатор мигает зеленым цветом с частотой 0,5 Гц.
4. Нажать и удерживать три секунды кнопку «М/ОК», отобразится меню прибора. С помощью кнопок «▲», «▼»,«◄», «►» выбрать пункт [**Тесты**], нажать на кнопку «М/ОК», выбрать пункт [**Все тесты**], нажать на кнопку «М/ОК».
5. Выполнить все шаги автотестирования, нажимая на кнопку «М/ОК».

Для предотвращения несанкционированного доступа к меню прибора необходимо зарегистрировать пользователя с правами администратора. Регистрацию можно осуществить по отпечатку пальца или паролю. Регистрация администратора может быть осуществлена через программу BAProg.

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 «BAProg» (см. далее).

Комплект поставки

В комплект поставки «С2000-BIOAccess-F18» входят:

- «С2000-BIOAccess-F18» – 1 шт.
- Паспорт – 1 экз.
- Инструкция по монтажу – 1 экз.
- Шаблон разметки для монтажа – 1 шт.
- Провода с разъёмами – 5 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.
- Резиновая прокладка кронштейна – 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 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 необходимо закрепить на кронштейне, зафиксировав его ранее откученными винтами.

ВНИМАНИЕ! 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 необходимо удалить защитные плёнки со сканера отпечатков пальцев и дисплея. При наклеенной защитной плёнке на сканере отпечатков пальцев не гарантируется их корректное распознавание.

Схемы электрических соединений

Подключение электрических цепей контроллера производится с помощью штырьковых разъёмов, расположенных на его задней стороне. Кабели с ответными частями данных разъёмов входят в комплект поставки. Во избежание неправильного подключения все разъёмы имеют разное число контактов, а разъём питания к тому же имеет отличную от остальных форму. Схема расположения разъёмов приведена на рис. 3.

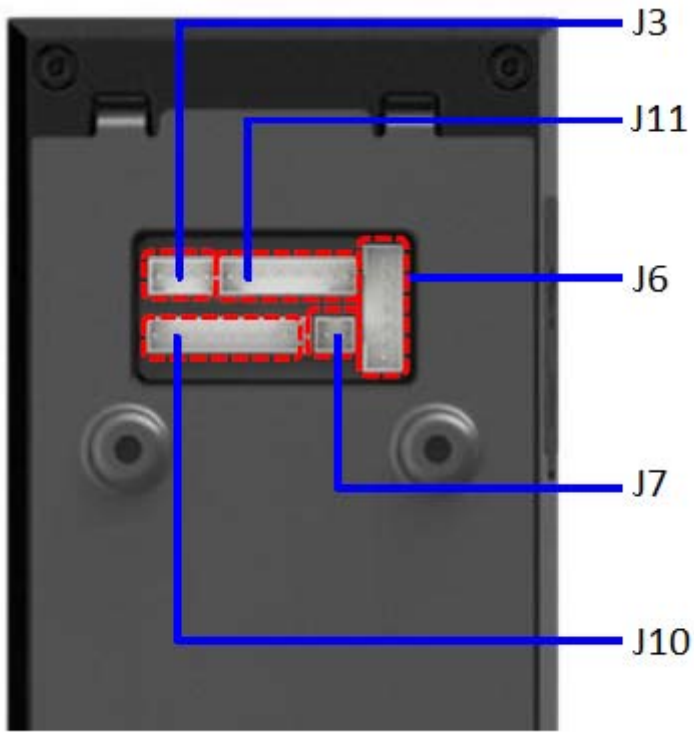


Рисунок 3. Схема расположения разъёмов

J3 – разъём Ethernet, 4 контакта;

J6 – разъём RS-232, RS-485, Wiegand (выход), 8 контактов;

J7 – разъём питания, 2 контакта;

J10 – разъём подключения замка, сирены, кнопки «Выход» и датчика двери, 10 контактов.

J11 – разъём для подключения внешнего считывателя , 7 контактов.

Таблица 3. Назначение и описание контактов разъёма J3

Номер контакта	Название	Назначение, цвет подсоединяемого провода
1	RJ45-1	RJ-45 – контакт 1, TX+, жёлтый
2	RJ45-2	RJ-45 – контакт 2, TX-, зелёный
3	RJ45-3	RJ-45 – контакт 3, RX+, красный
4	RJ45-6	RJ-45 – контакт 6, RX-, чёрный

Таблица 4. Назначение и описание контактов разъёма J6

Номер контакта	Название	Назначение, цвет подсоединяемого провода
1	WD0-OUT	Wiegand – данные «0», зелёный
2	WD1-OUT	Wiegand – данные «1», белый
3	GND	Wiegand – GND, чёрный
4	RXD*	RS-232 – RXD, серый
5	TXD*	RS-232 – TXD, фиолетовый
6	GND*	RS-232 – GND, чёрный
7	485A*	RS-485 – линия A, синий
8	485B*	RS-485 – линия B, жёлтый

* – неиспользуемые в текущей версии контроллера контакты

Таблица 5. Назначение и описание контактов разъёма J7

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

Таблица 6. Назначение и описание контактов разъёма J10

Номер контакта	Название	Назначение, цвет подсоединяемого провода
1	BELL-	Звонок-, фиолетовый
2	BELL+	Звонок+, коричневый
3	SENSOR	Датчик двери, белый
4	GND	GND кнопки «Выход» и датчика дверей, чёрный
5	BUTTON	Кнопка «Выход», серый
6	NO	Реле замка, нормально-разомкнутый контакт, голубой
7	COM	Реле замка, общий контакт, красный
8	NC	Реле замка, нормально-замкнутый контакт, желтый
9	ALARM-	Сирена-, оранжевый
10	ALARM+	Сирена+, зеленый

Таблица 7. Назначение и описание контактов разъёма J11

Номер контакта	Название	Назначение, цвет подсоединяемого провода
1	12V-OUT*	Питание внешнего считывателя +12 В, красный
2	GND*	Питание внешнего считывателя GND, черный
3	D0-IN*	Внешний считыватель – Wiegand – данные «0», белый
4	D1-IN*	Внешний считыватель – Wiegand – данные «1», зеленый
5	RLED*	Индикация – красный светодиод, синий
6	GLED*	Индикация – зелёный светодиод, серый
7	BEEP*	Индикация – звуковой сигнализатор, фиолетовый

* – неиспользуемые в текущей версии контроллера контакты

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/демонтажом 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.

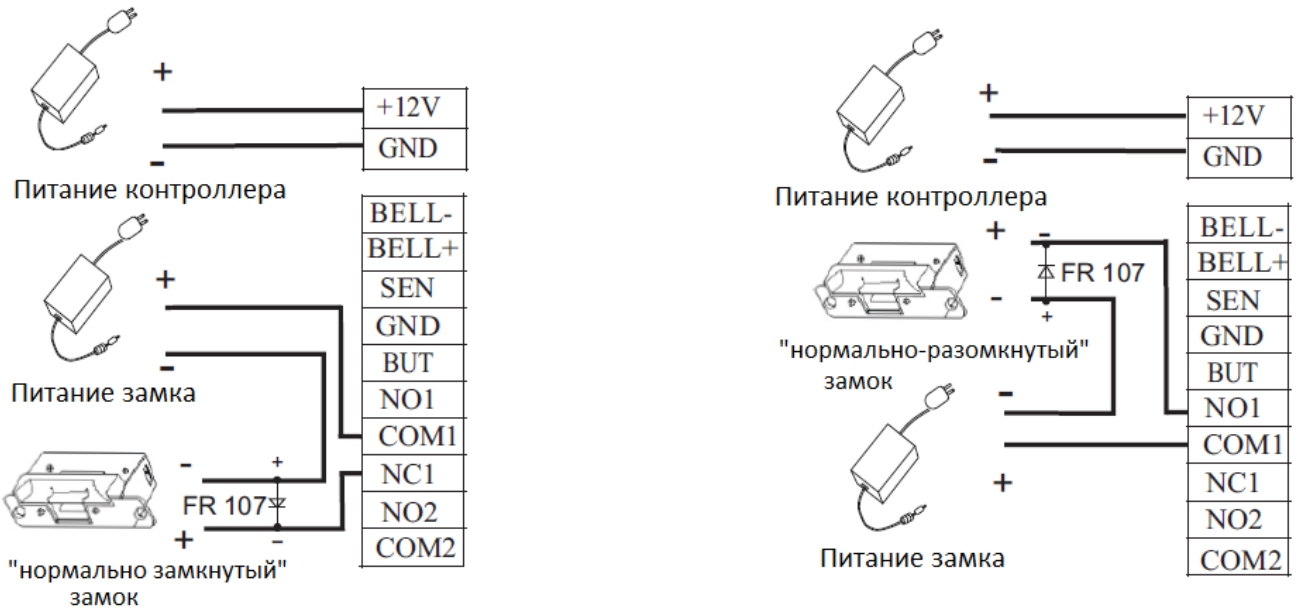


Рисунок 4. Рекомендуемые схемы подключения замков (разъём J10)

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 BAProg.

Некоторые параметры можно отредактировать только через меню контроллера. Через меню контроллера может потребоваться изменить, например, следующие параметры:

- тип датчика двери;
- сигнализация блокировки открытой двери;
- включение сигнала тревоги;
- блокировка кнопки включения/выключения питания.

После настройки в BAProg (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.

Настройки, осуществляемые через меню контроллера

Внимание! В данном руководстве приводится описание только тех пунктов приборного меню, которые необходимы для настройки контроллера при его совместной работе с системой ОРИОН-ПРО, а также при автономной работе с утилитой настройки BAProg.

Во избежание приведения прибора в неработоспособное состояние, категорически запрещается работать с экранами и пунктами меню контроллера, которые не описаны в настоящем руководстве.

Вход в меню контроллера

Для входа в меню нужно нажать на кнопку «M.Ok» и удерживать ее в нажатом состоянии 3 сек. Если в контроллере не зарегистрировано пользователей с правами администратора, то на дисплее появятся пункты меню.

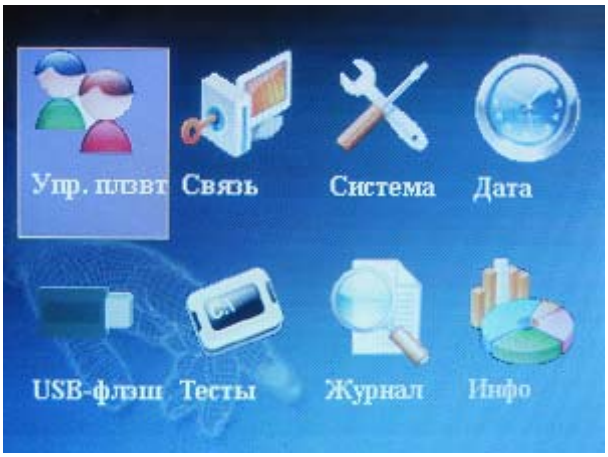


Рисунок 5. Главное меню контроллера

Выбор нужного пункта меню осуществляется при помощи кнопок со стрелками «▲», «▼». Для перехода на уровень ниже или выбора пункта меню нужно нажать на кнопку «М/ОК». Переход на уровень выше осуществляется по нажатию на кнопку «С».

Если в контроллере зарегистрирован пользователь с правами администратора, то после удержания кнопки «М/ОК» на дисплее высветится окно с изображением замка и надписи в верхнем левом углу «Адм.права» + номер сотрудника-администратора (на рис. он имеет номер 1)

Рисунок 6. Экран авторизации при входе в меню контроллера

Если тип пароля администратора - proximity карта, то для входа в меню необходимо и достаточно приложить карту администратора.

Если тип пароля - отпечаток пальца, то для входа в меню необходимо и достаточно приложить палец администратора.

Если тип пароля администратора - цифровой код, то необходимо проделать следующие действия:

- на клавиатуре прибора необходимо набрать указанный номер сотрудника-администратора, после чего автоматически отобразится следующий экран, на котором надо снова ввести идентификатор (номер) сотрудника-администратора и нажать кнопку «М/ОК»

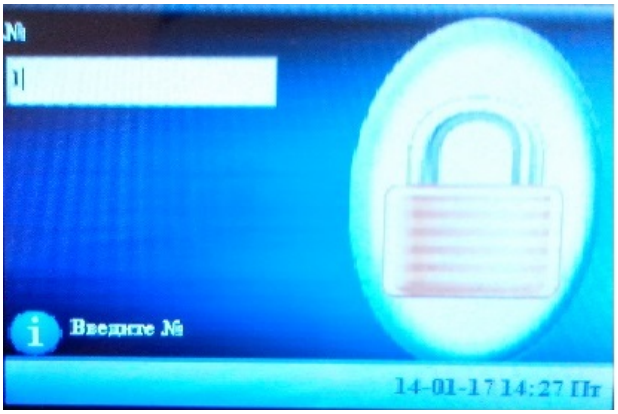


Рисунок 7. Экран ввода идентификатора сотрудника

- после ввода идентификатора на следующем экране необходимо ввести пароль администратора и нажать кнопку «М/ОК»

Рисунок 8. Экран ввода пароля

Контроллер проверит пароль, и, если он введен корректно, отобразит главное приборное меню (см. Рисунок 5).

Подключение к ПК

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

На рис. 9, 10 приведены схемы подключения контроллеров по интерфейсу Ethernet.

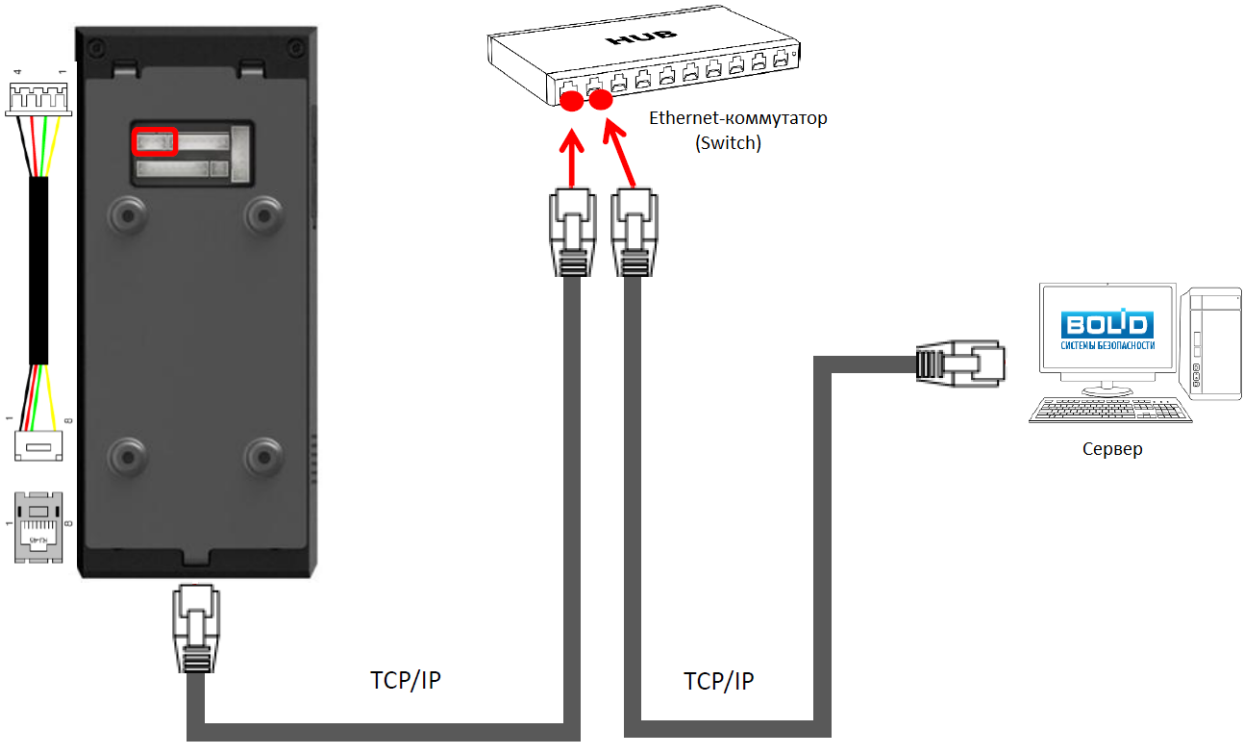


Рисунок 9. Подключение контроллера к ПК через Ethernet-коммутатор (Switch)

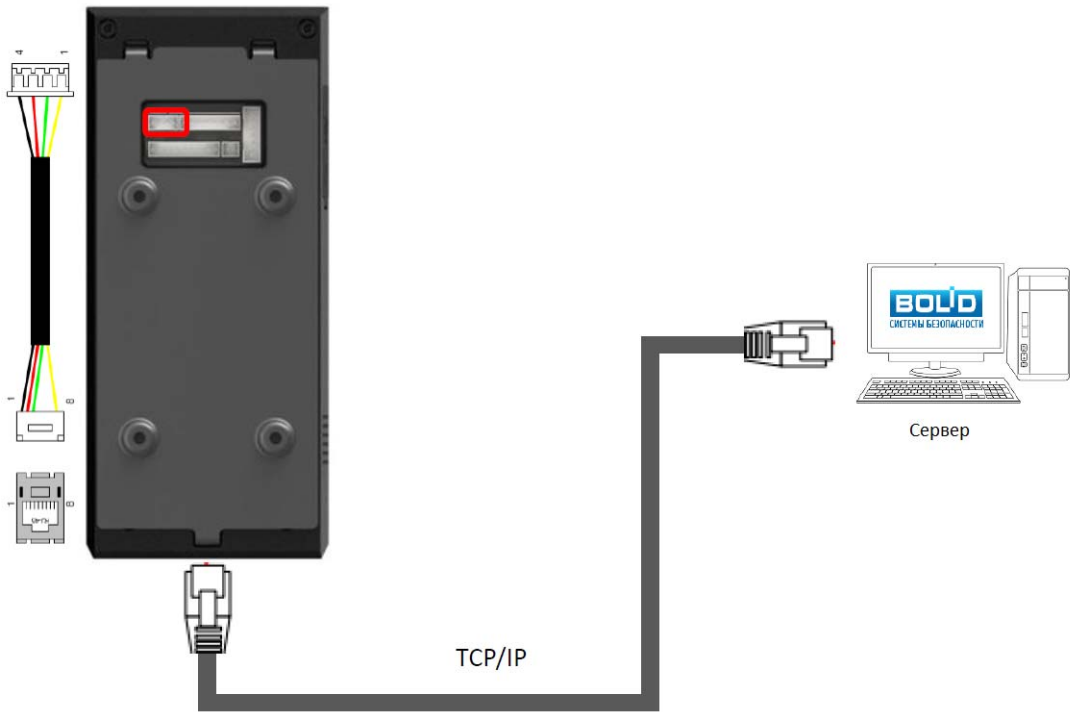


Рисунок 10. Подключение контроллера к ПК напрямую

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.

Настройка уникального идентификатора (номера устройства)

Для корректной работы в составе системы ОРИОН-ПРО каждый биометрический контроллер должен иметь уникальный идентификатор (номер устройства). По умолчанию этот номер равен 1. Для установки идентификатора необходимо выполнить следующую последовательность действий:

1. Войти в главное меню прибора (см. предыдущий пункт Руководства)

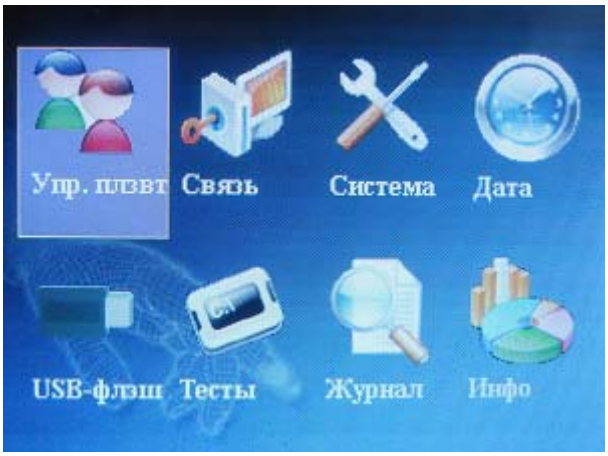


Рисунок 11. Главное меню прибора

2. Выбрать пункт «Связь»
3. Выбрать пункт «Безопасн.»

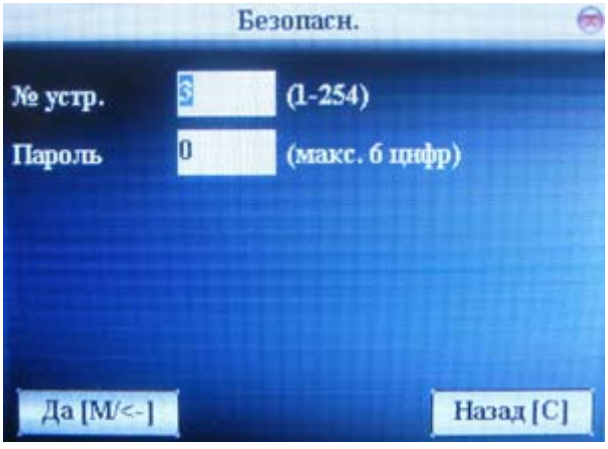


Рисунок 12. Меню «Безопасность»

4. Ввести значение идентификатора в окошко «№ устр.» (от 1 до 254)
5. Нажать на кнопку «М/ОК» для сохранения параметра в постоянной памяти устройства.

После появления окошка с надписью «Изменения сохранены» еще раз нажать «М/ОК».

Настройка параметров сети

Для корректной работы в составе системы ОРИОН-ПРО необходимо задать параметры сетевого подключения. По умолчанию IP-адрес прибора установлен в **192.168.1.201**, а маска подсети имеет значение **255.255.255.0**. Для установки сетевых параметров необходимо выполнить следующую последовательность действий:

1. Войти в главное меню прибора (см. предыдущий пункт Руководства)

Рисунок 13. Главное меню прибора

2. Выбрать пункт «**Связь**»

Рисунок 14. Меню «Связь»

3. Выбрать пункт «**Сеть**»

Рисунок 15. Меню «Сеть»

Ввести значение параметров «**IP адрес**», «**Маска сети**» и «**Шлюз**» (при необходимости)

Нажать на кнопку «М/ОК» для сохранения параметра в постоянной памяти устройства.

После появления окошка с надписью «Изменения сохранены» еще раз нажать «М/ОК».

Выбор типа датчика двери

Цепь датчика двери может быть нормально разомкнутой или нормально замкнутой.

Для выбора типа датчика двери нужно выполнить следующую последовательность действий:

1. Войти в главное меню прибора (см. соответствующий пункт Руководства)
2. Выбрать пункт «**Упр.плзвт**»
3. Выбрать пункт «**Доступ**»

Рисунок 16. Меню «Управление пользователями»

4. Выбрать пункт «**Настр. контр. доступ**а»

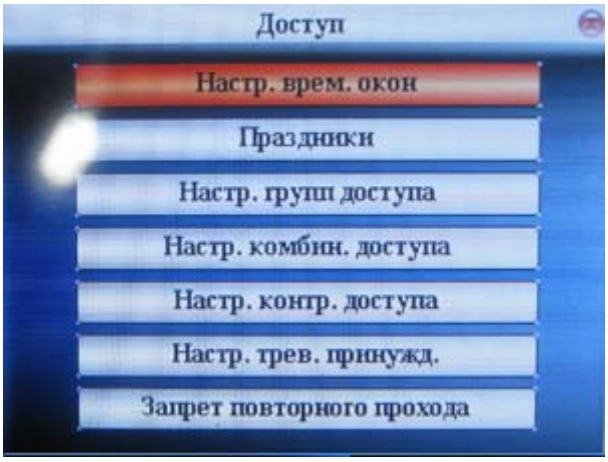


Рисунок 17. Меню «Доступ»

5. Перейти на пункт «**Режим СМК**»

Рисунок 18. Меню «Настройки контроля доступа»

Выбрать при помощи клавиш со стрелками «<» и «>» нужное значение из списка возможных:

- «**Откр**» - нормально разомнутый

- «**Закр**» - нормально замкнутый

- «**Нет**» датчик двери не используется

Нажать на кнопку «М/ОК» для сохранения параметра в постоянной памяти устройства.

После появления окошка с надписью «Изменения сохранены» еще раз нажать «М/ОК».

Настройка включения сигнализации при блокировке двери

В случае блокировки открытой двери может включаться сигнал тревоги. Для установки времени, через которое включается сигнал тревоги при блокировке открытой двери, нужно выполнить следующие действия:

1. Войти в приборное меню (см. пункт выше)
2. Выбрать пункт «**Упр.плзвт**»
3. Выбрать пункт «**Доступ**»

Рисунок 19. Главное меню прибора

4. Выбрать пункт «**Настр. контр. доступа**»

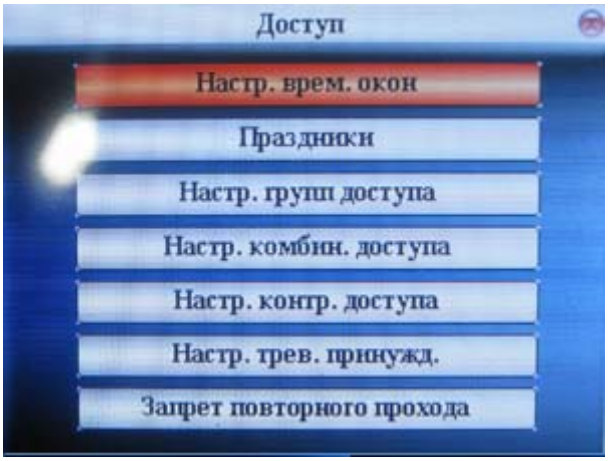


Рисунок 20. Меню «Доступ»

5. Перейти на пункт «**Задерж трев**» кнопками со стрелками

Рисунок 21. Меню «Настройки контроля доступа»

Ввести время в секундах (от 1 до 99). Если установлено значение параметра «0», то сигнал тревоги не включается.

Нажать на кнопку «М/ОК» для сохранения параметра в постоянной памяти устройства.

После появления окошка с надписью «Изменения сохранены» еще раз нажать «М/ОК».

Настройка включения сигнала тревоги в случае неудачной аутентификации

В случае нескольких попыток неудачной аутентификации подряд (например, несколько раз подряд введён неверный пароль) может быть включён сигнал тревоги. Для выбора количества неудачных попыток получения доступа, при котором включается сигнал тревоги, нужно выполнить следующие действия:

1. Войти в приборное меню (см. пункт выше)
2. Выбрать пункт «**Упр.плзвт**»
3. Выбрать пункт «**Доступ**»

Рисунок 22. Главное меню прибора

4. Выбрать пункт «**Настр. контр. доступ**а»

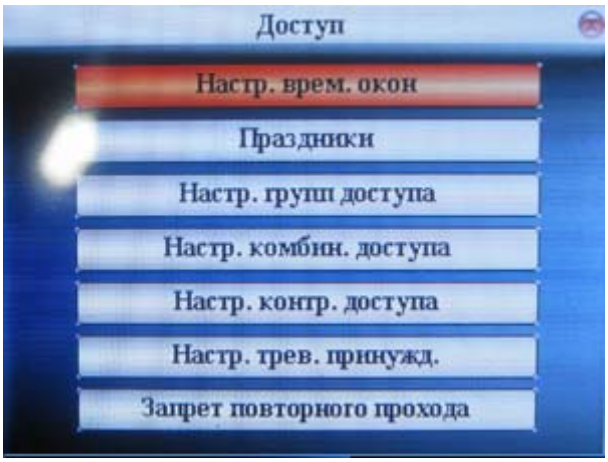


Рисунок 23. Меню «Доступ»

5. Перейти на пункт «**Сч. тревог**» кнопками со стрелками

Рисунок 24. Меню «Настройки контроля доступа»

Указать количество попыток (1 до 9). Если установлено значение параметра «0», то сигнал тревоги не включается.

Нажать на кнопку «М/ОК» для сохранения параметра в постоянной памяти устройства.

После появления окошка с надписью «Изменения сохранены» еще раз нажать «М/ОК».

BAProg

Программа BAProg используется для конфигурирования «C2000-BIOAccess-F18».

Установка BAProg

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

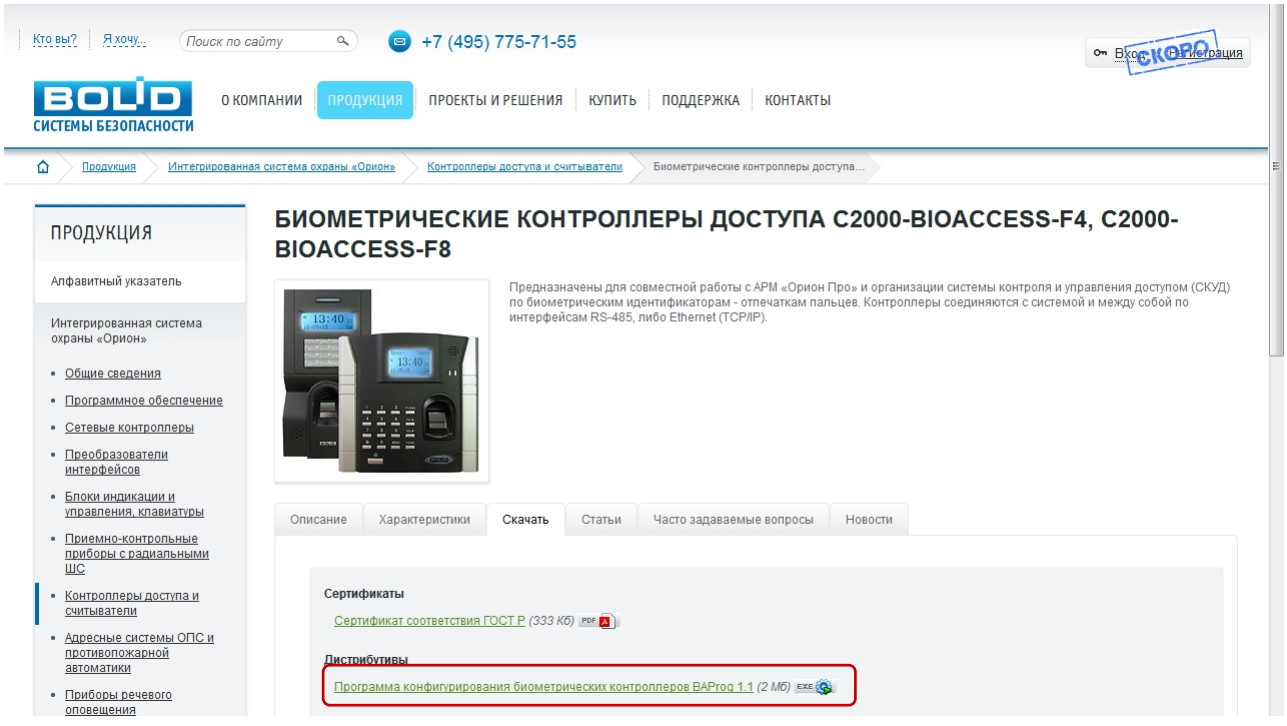


Рисунок 25

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 или Windows 7.

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

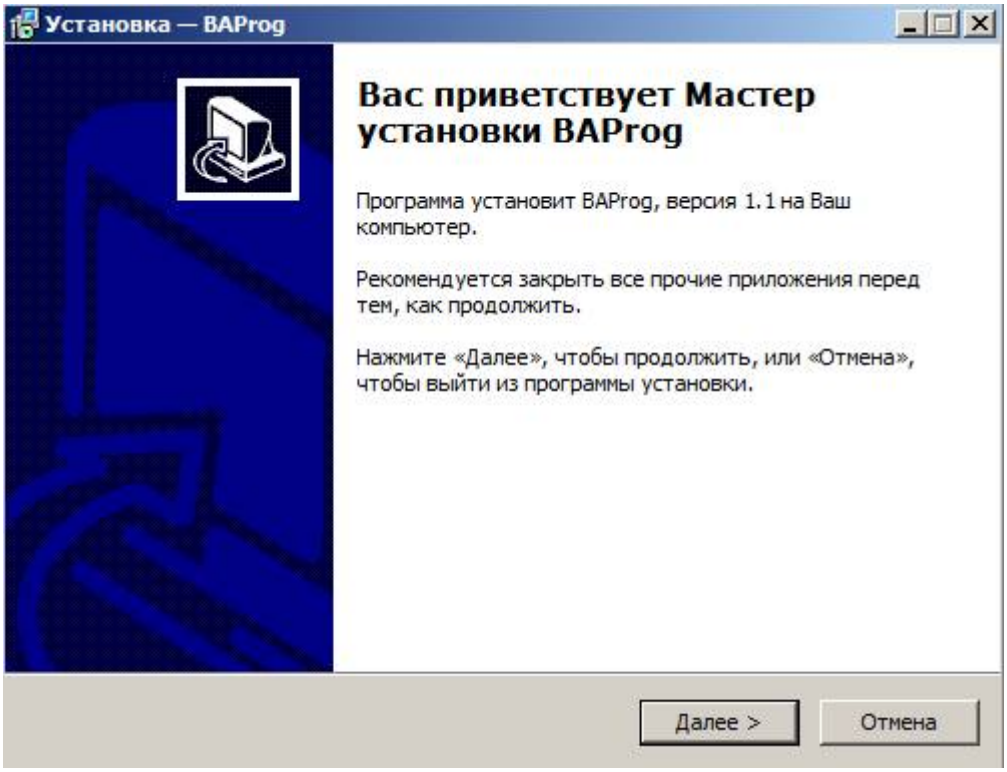


Рисунок 26

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

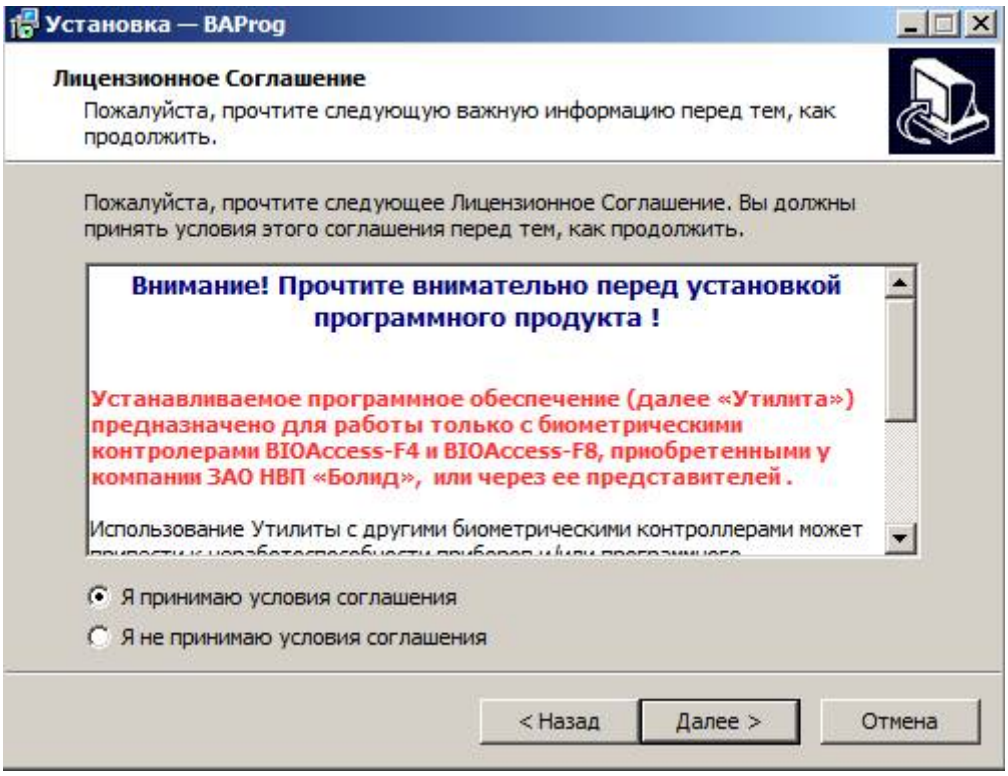


Рисунок 27

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

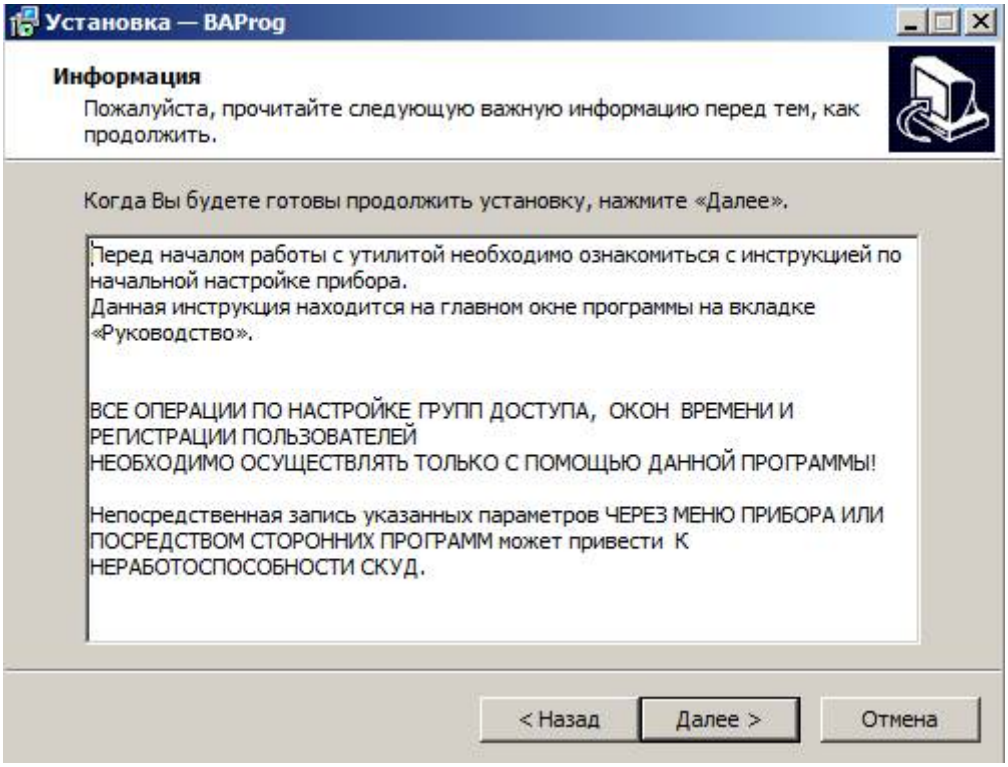


Рисунок 28

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

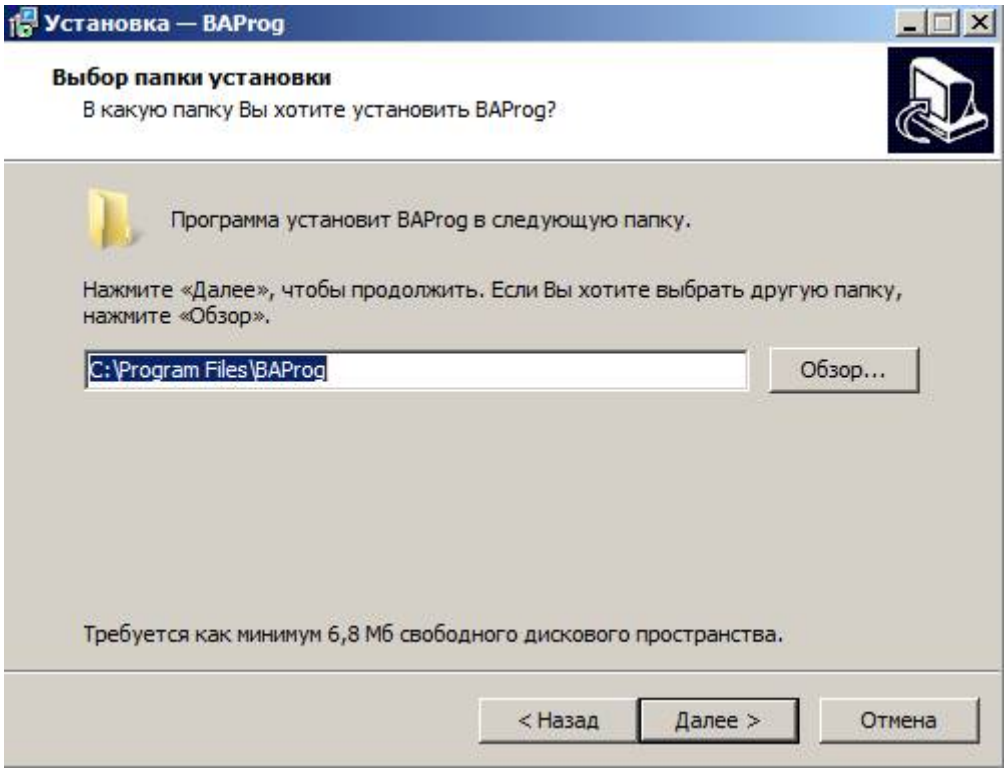


Рисунок 29

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

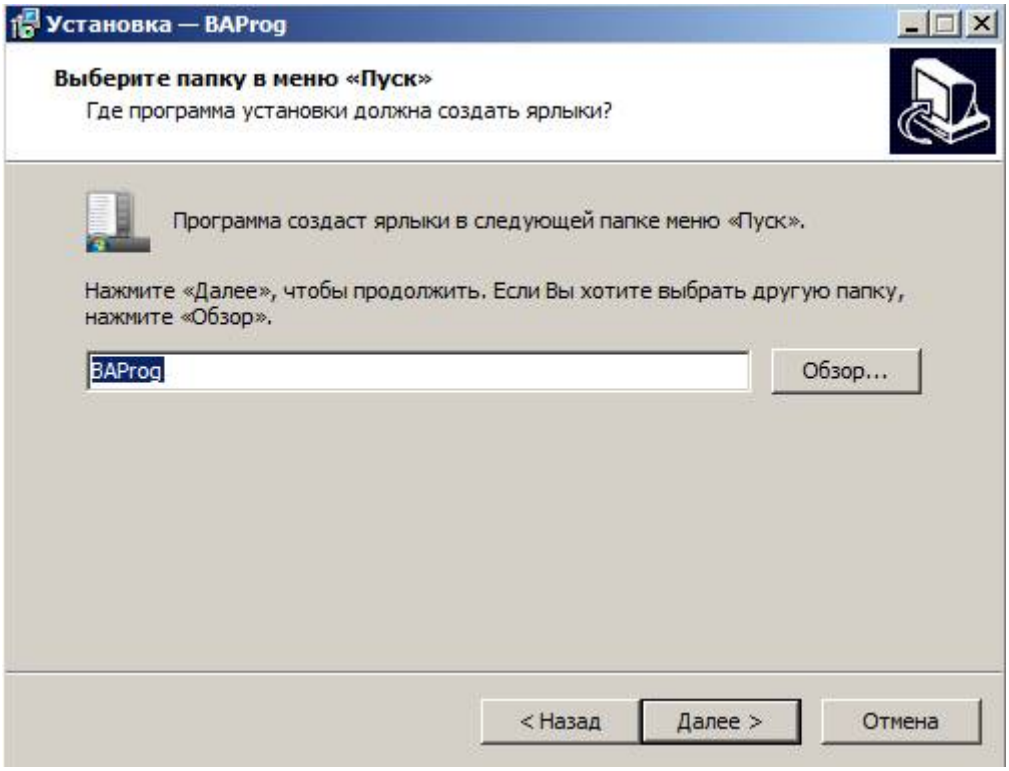


Рисунок 30

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

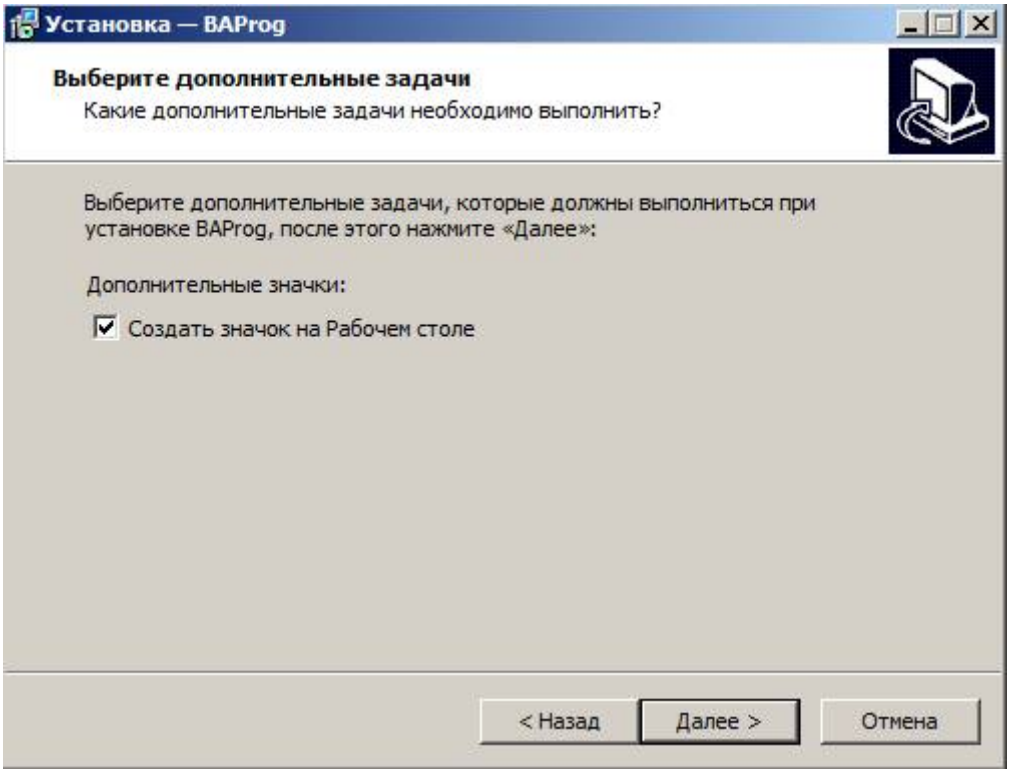


Рисунок 31

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

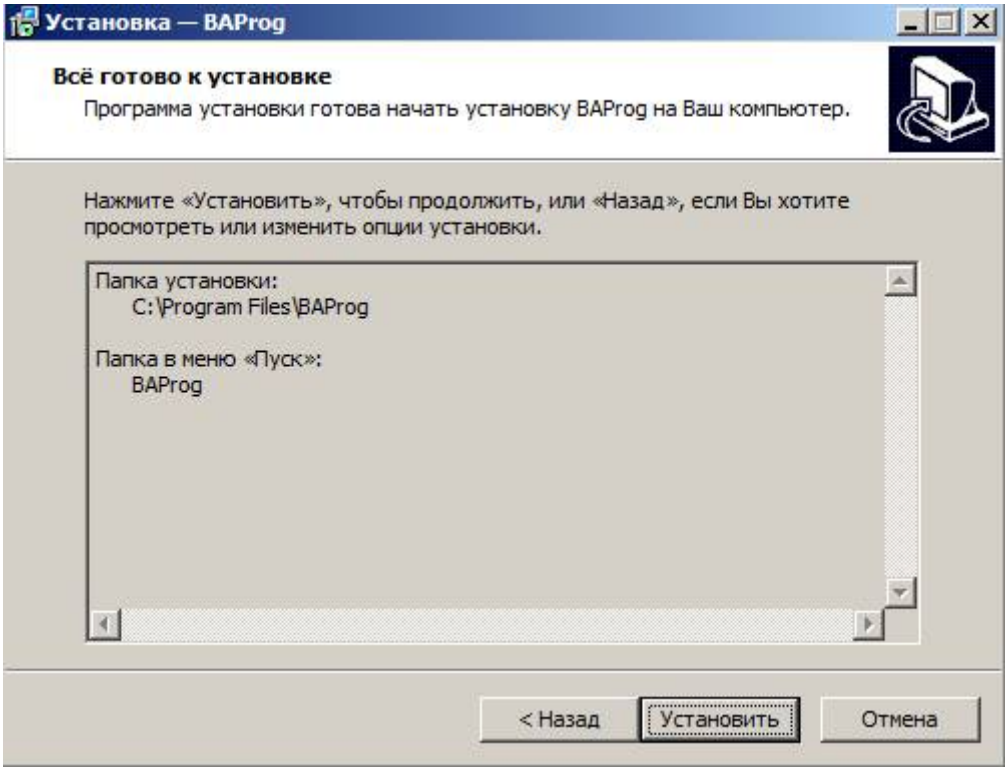


Рисунок 32

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.

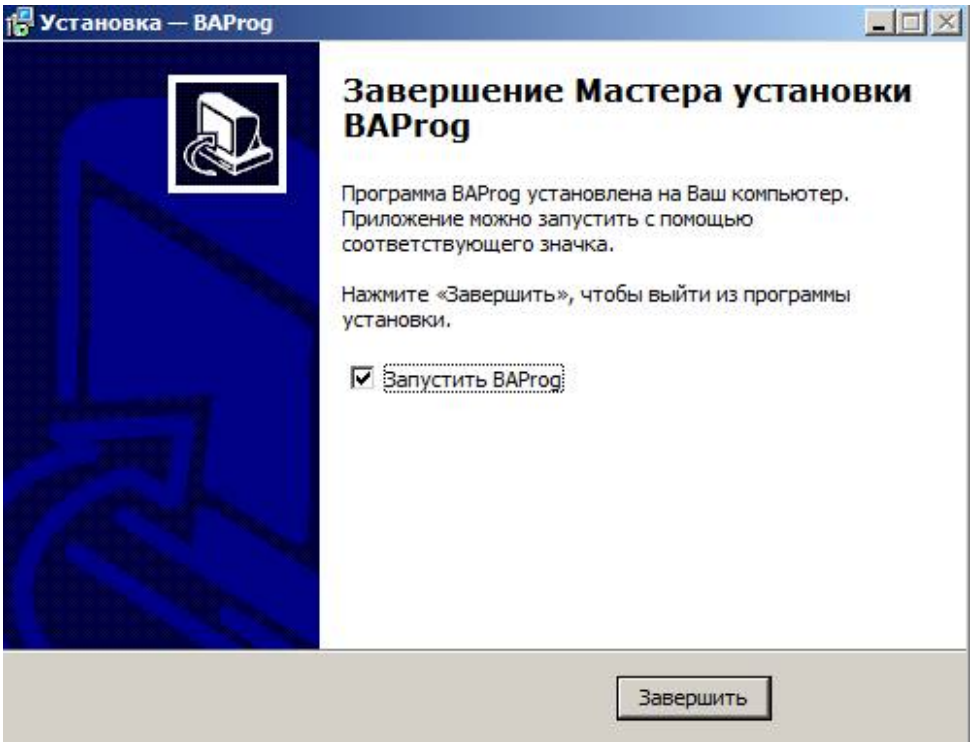


Рисунок 33

Интерфейс BAProg

При запуске окно BAProg выглядит следующим образом:

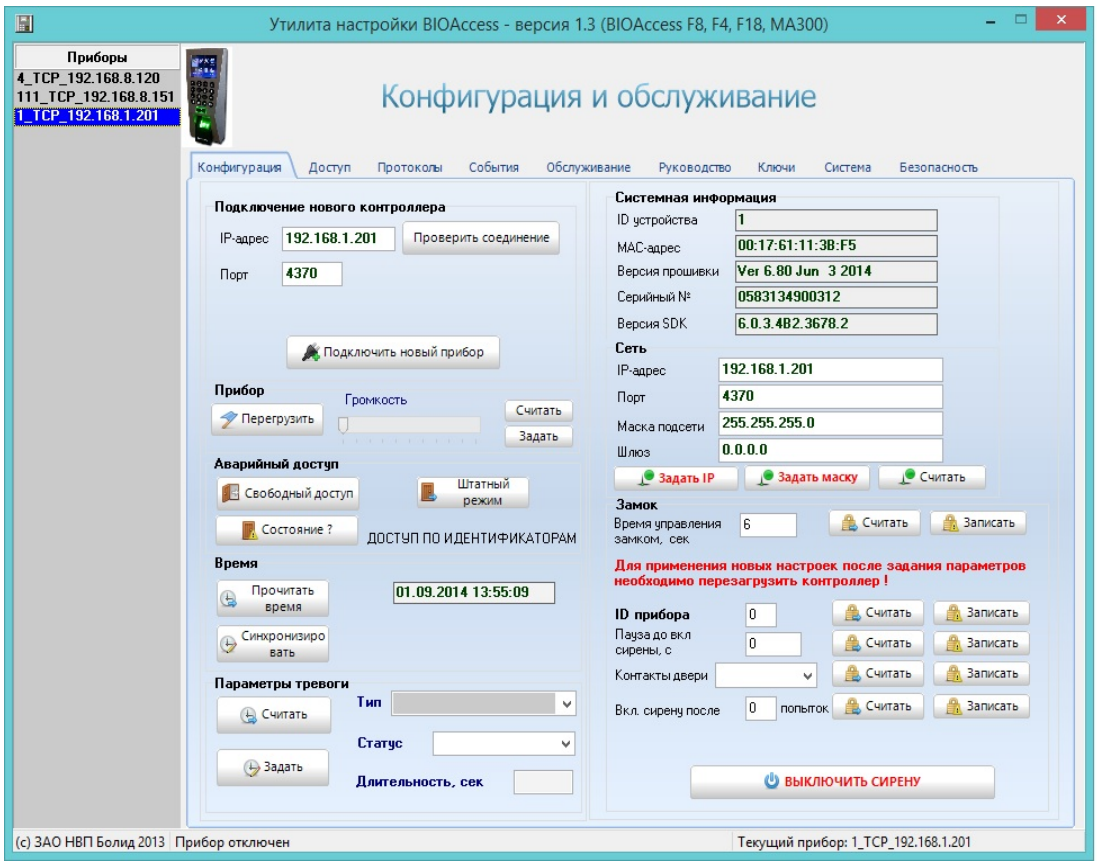


Рисунок 34

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

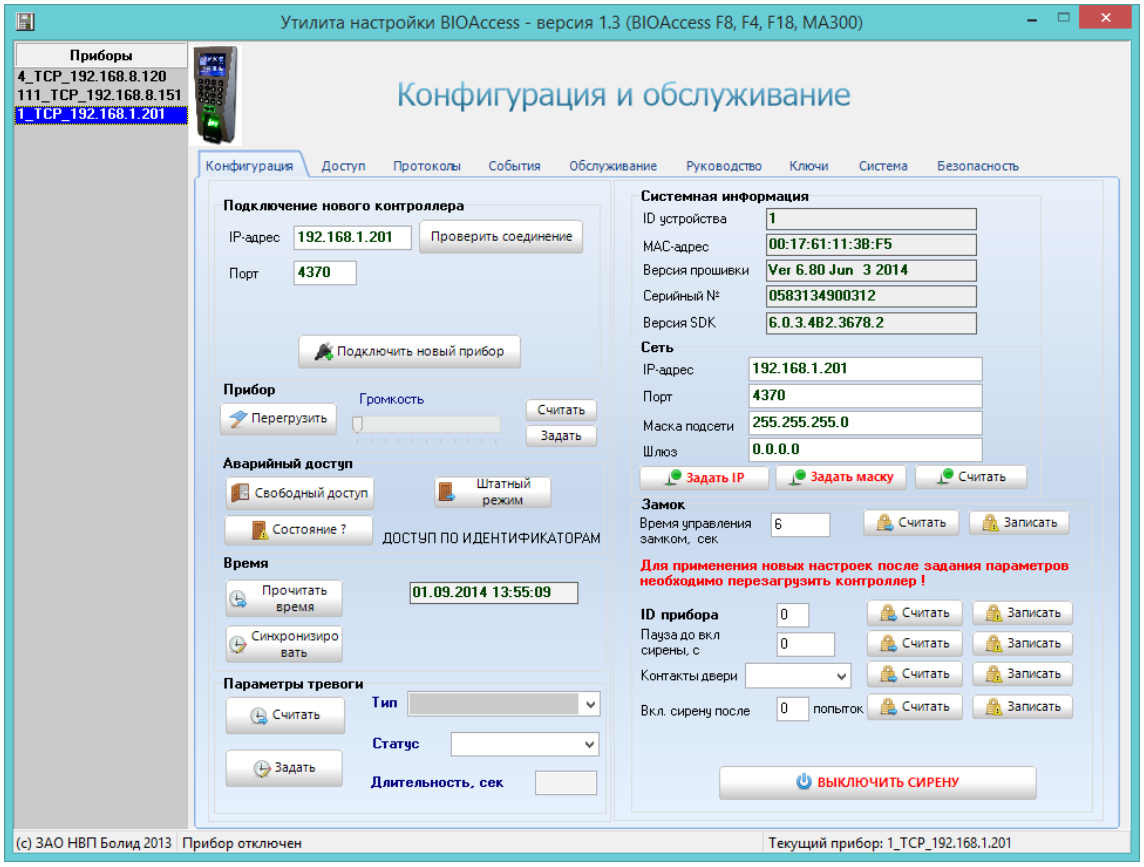


Рисунок 35

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.

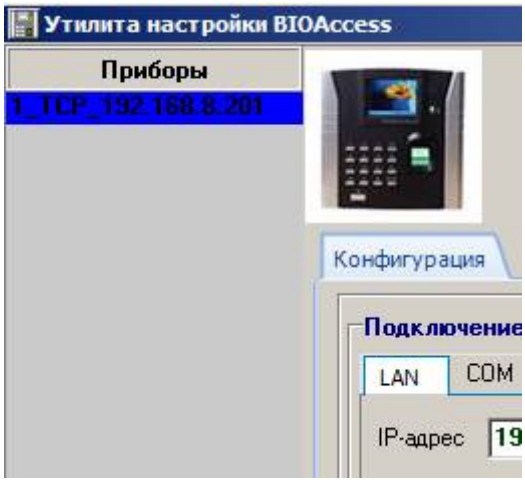


Рисунок 36

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. Пр 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.

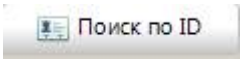
В поле «Замок» можно редактировать время управления замком. Установленное в контроллере время управления замком можно увидеть при нажатии на кнопку «Считать». Новое значение, указываемое в строке «Время управления замком, сек», можно записать с помощью кнопки «Записать».

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.

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.

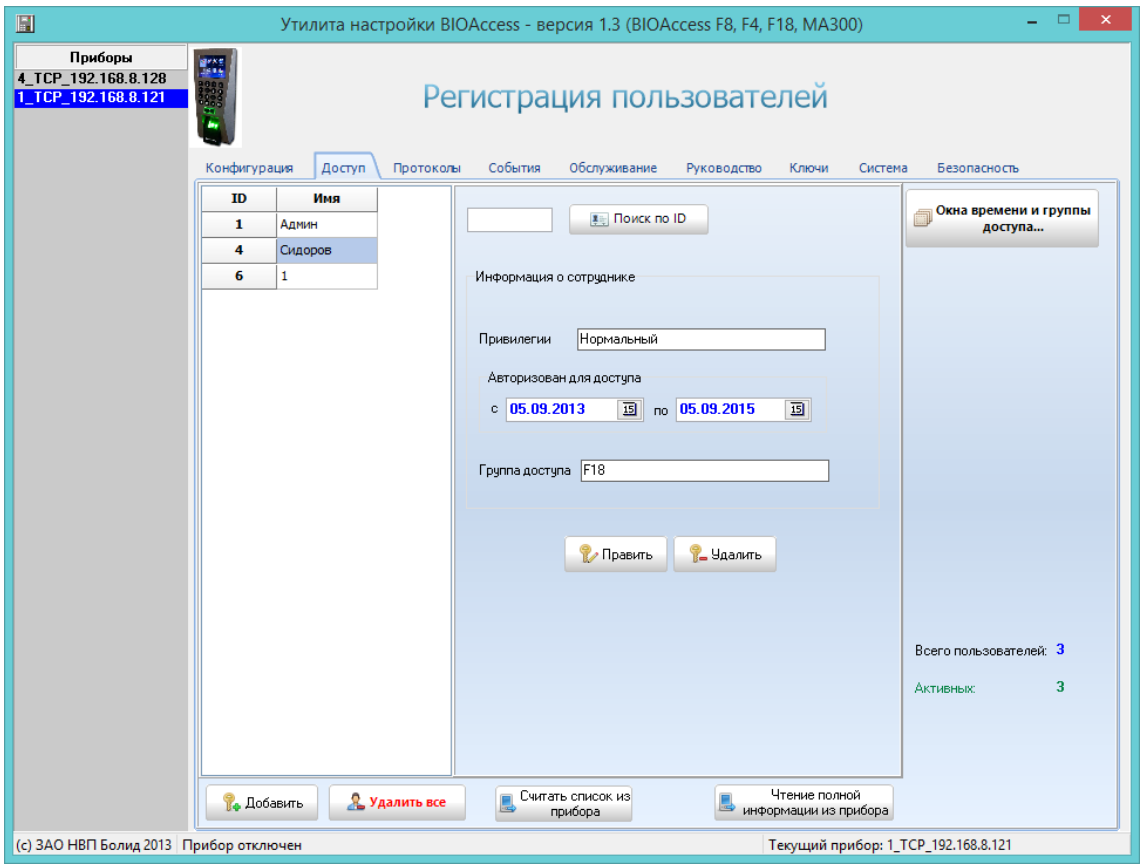
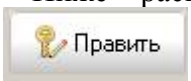
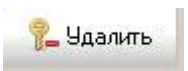


Рисунок 37

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:

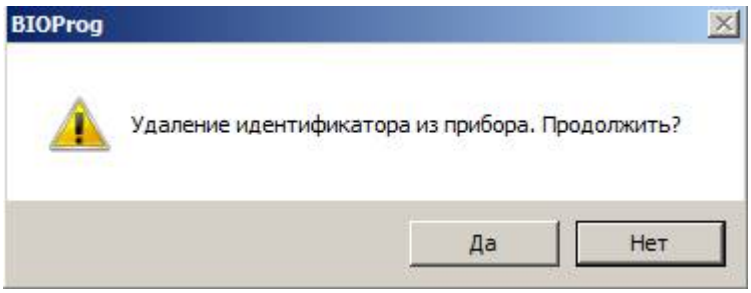
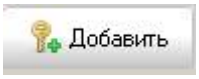


Рисунок 38

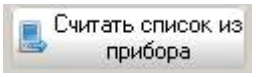
Для удаления информации о пользователе нужно нажать на кнопку «Да».

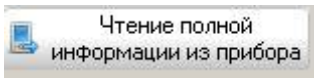
Также на вкладке «Доступ» показывается общее количество пользователей («Всего пользователей») и количество активных пользователей («Активных»).

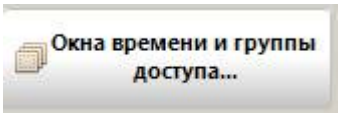
На этой же вкладке расположены кнопки:

- 

– 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:

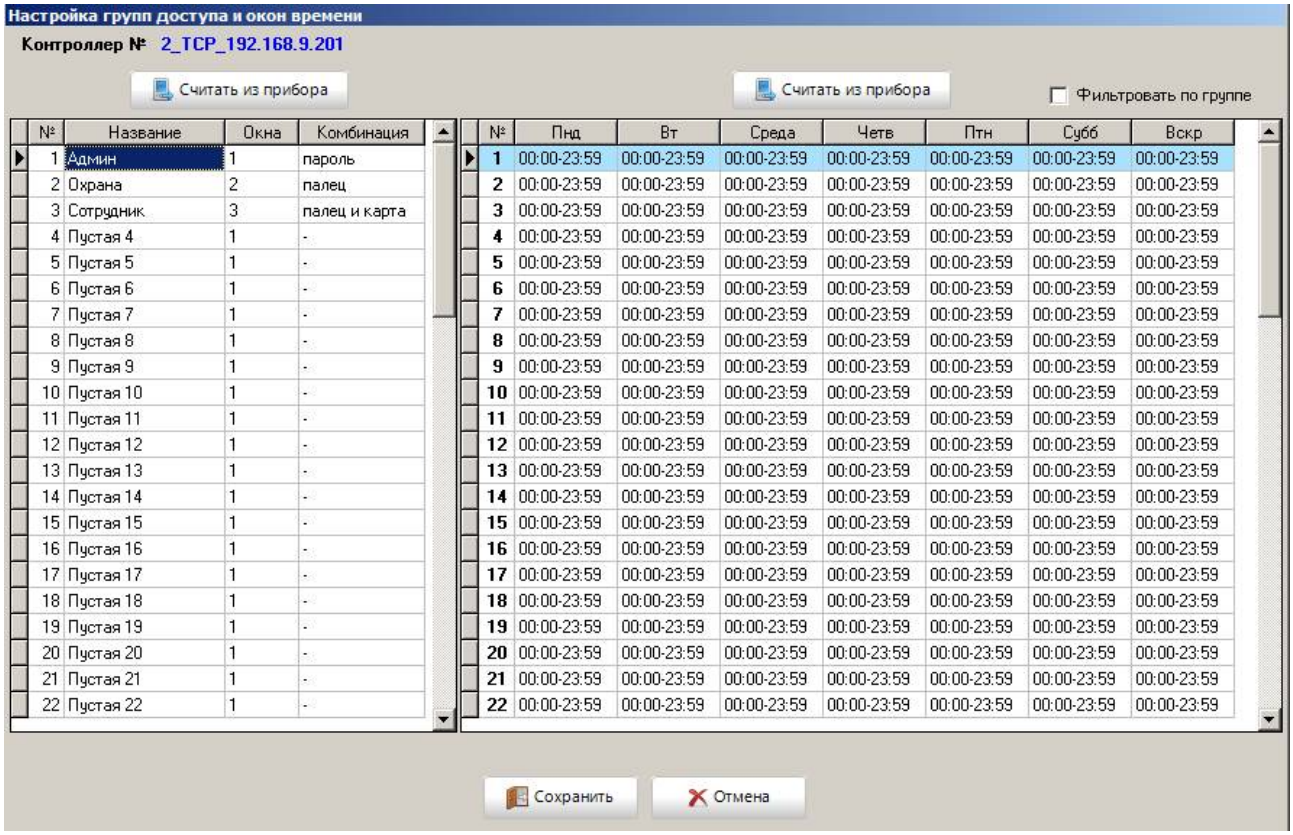
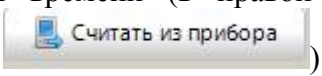


Рисунок 39

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»:

Рисунок 40

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»:

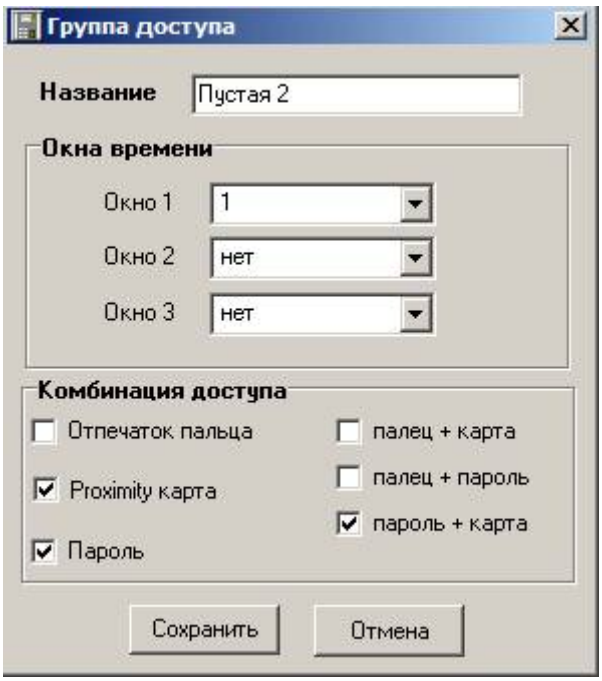


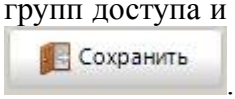
Рисунок 41

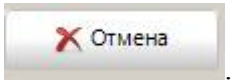
В этом окне можно указать «Название группы». В поле «Окна времени» выбираются необходимые для группы доступа окна времени. С помощью выпадающих списков «Окно 1», «Окно 2» и «Окно 3» можно выбрать до трёх окон времени.

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

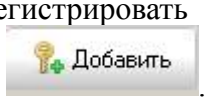
- отпечаток пальца
- Proximity карта
- пароль
- палец + карта
- палец + пароль
- палец + карта

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»):

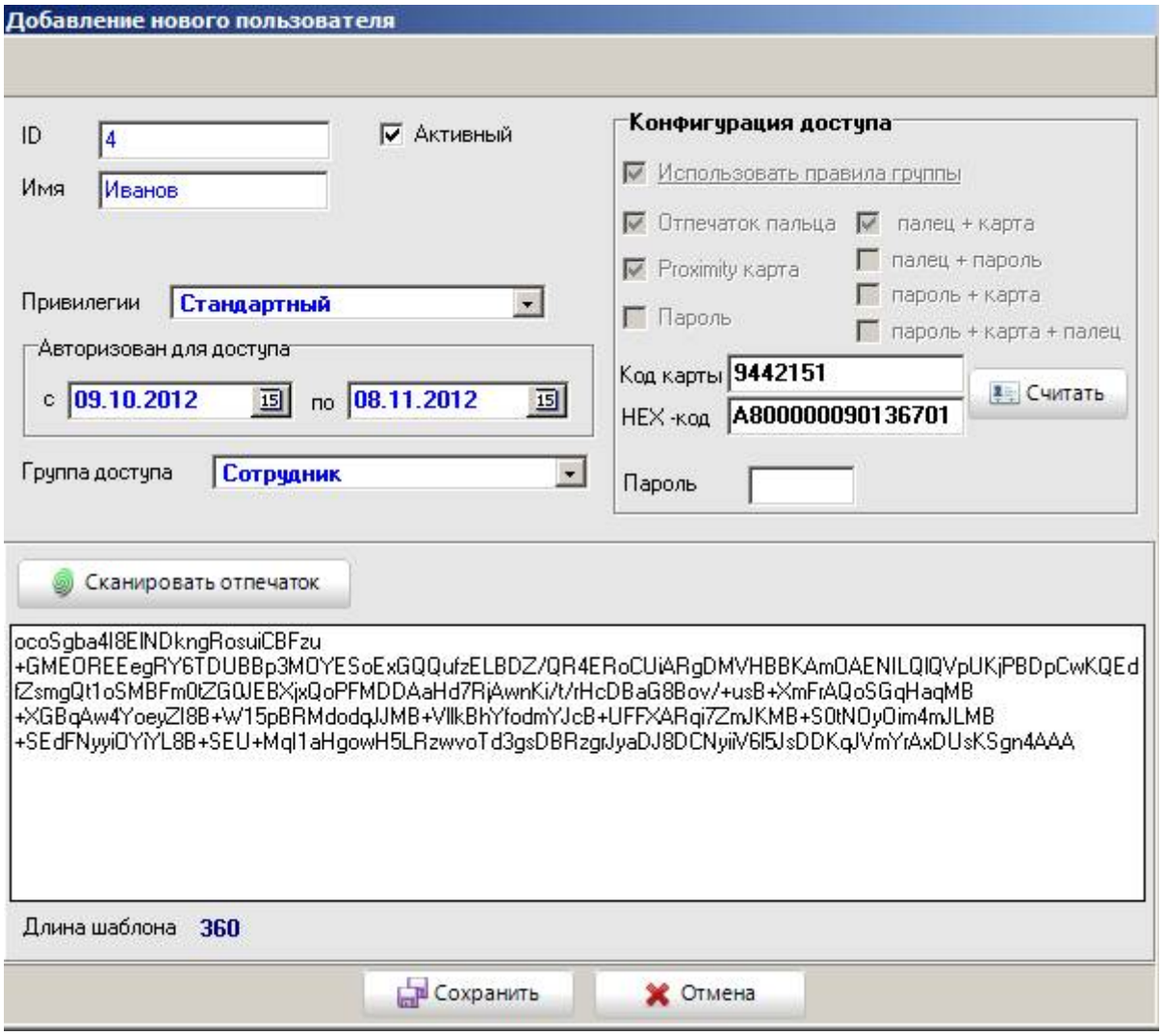


Рисунок 42

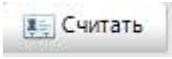
В этом окне указываются порядковый номер пользователя в общем списке пользователей (ID), имя пользователя (Имя). Имя должно содержать не более 8 символов. Опция «Активный» при отключении позволяет запретить доступ для зарегистрированного пользователя.

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

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

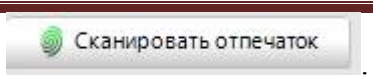
В списке «Группа доступа» выбирается необходимая группа доступа. Когда группа доступа выбрана, в поле «Конфигурация доступа» показываются настройки способа аутентификации для выбранной группы.

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.

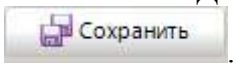
Для регистрации пароля нужный пароль нужно ввести в поле «Пароль».

Для сканирования отпечатка пальца нужно нажать на кнопку 

. При этом появляется сообщение:

Рисунок 43

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 прибора»

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

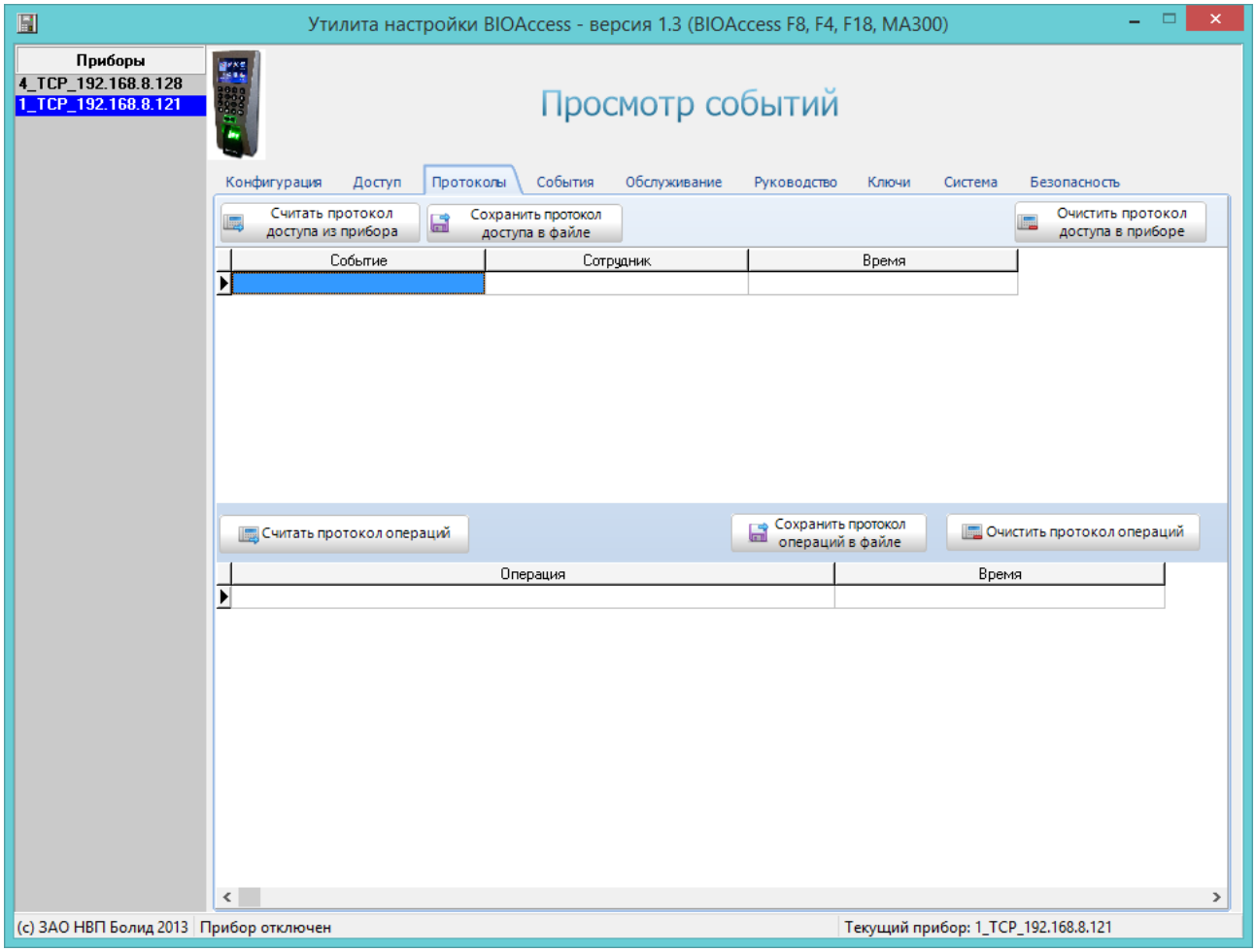
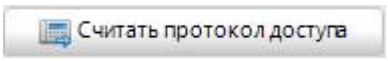
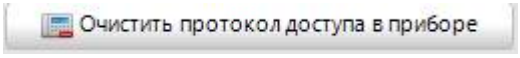
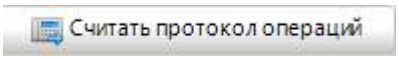


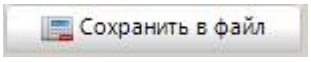
Рисунок 44

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:

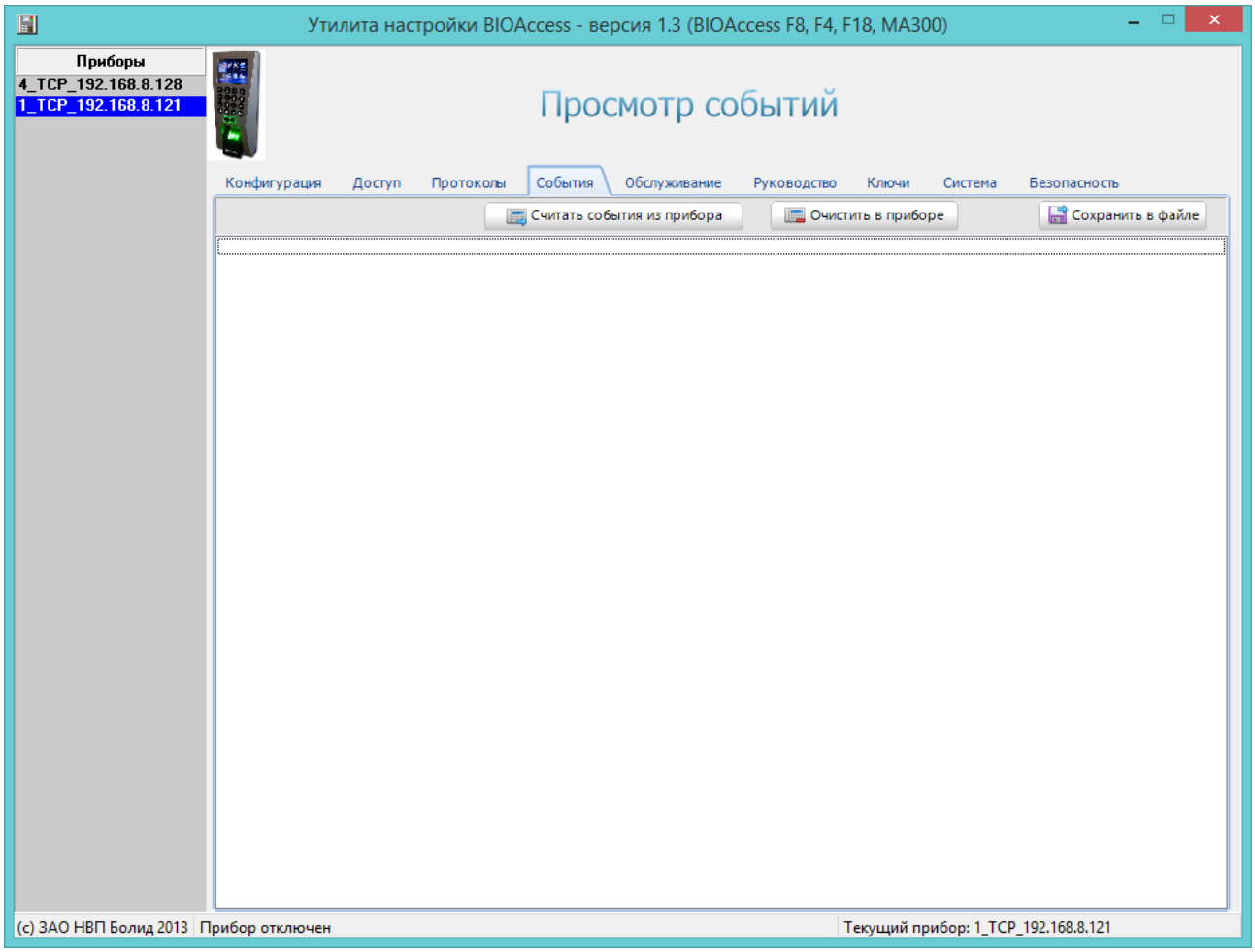
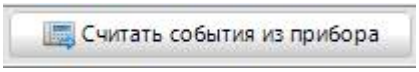
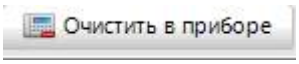
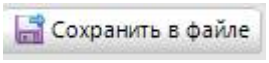


Рисунок 45

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.

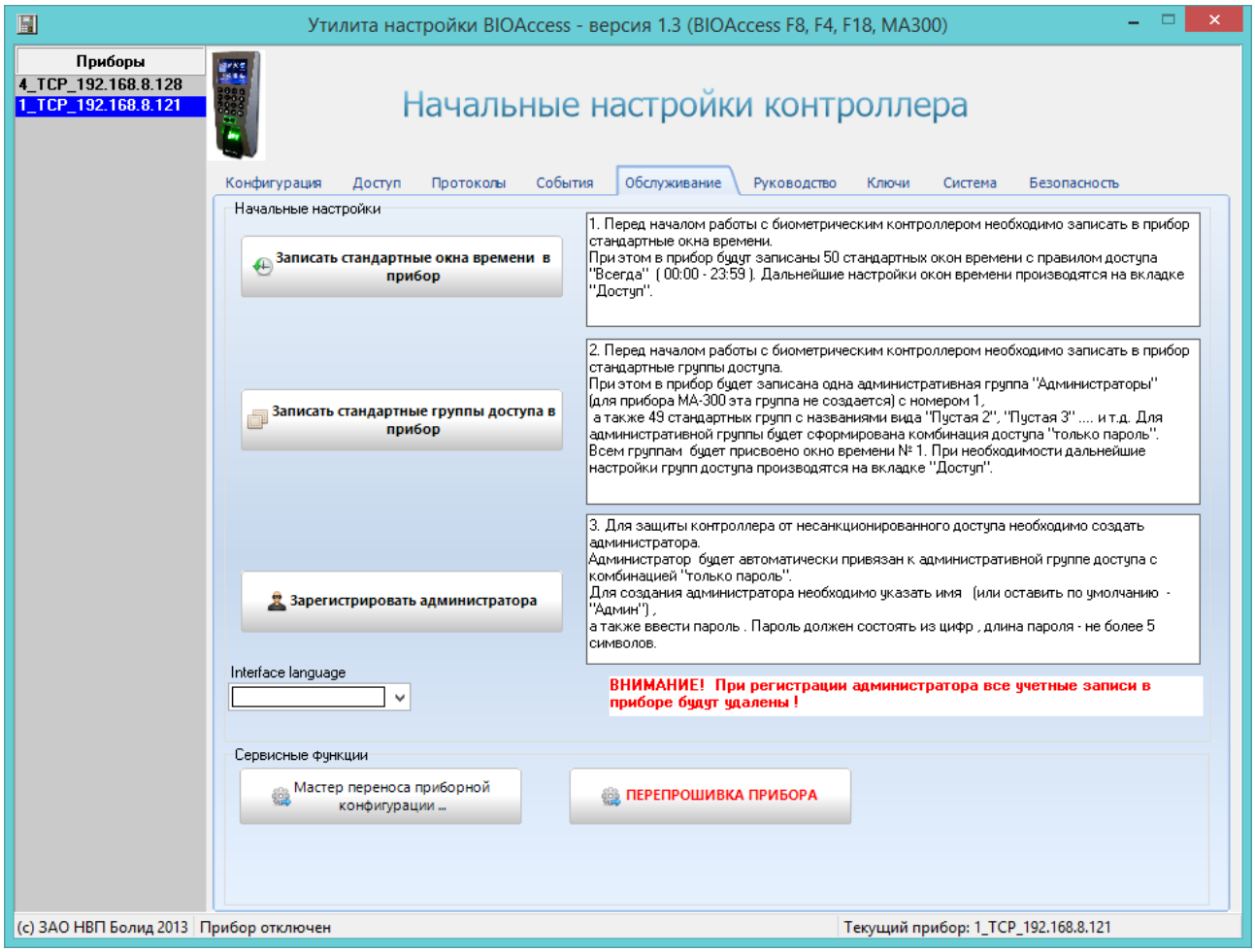
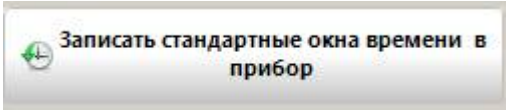
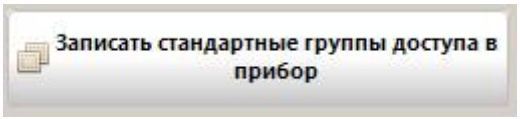
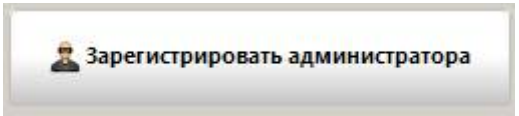


Рисунок 46

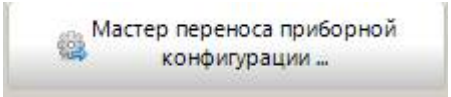
Начальные настройки контроллера осуществляются при нажатии на следующие кнопки:

- 

– 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:

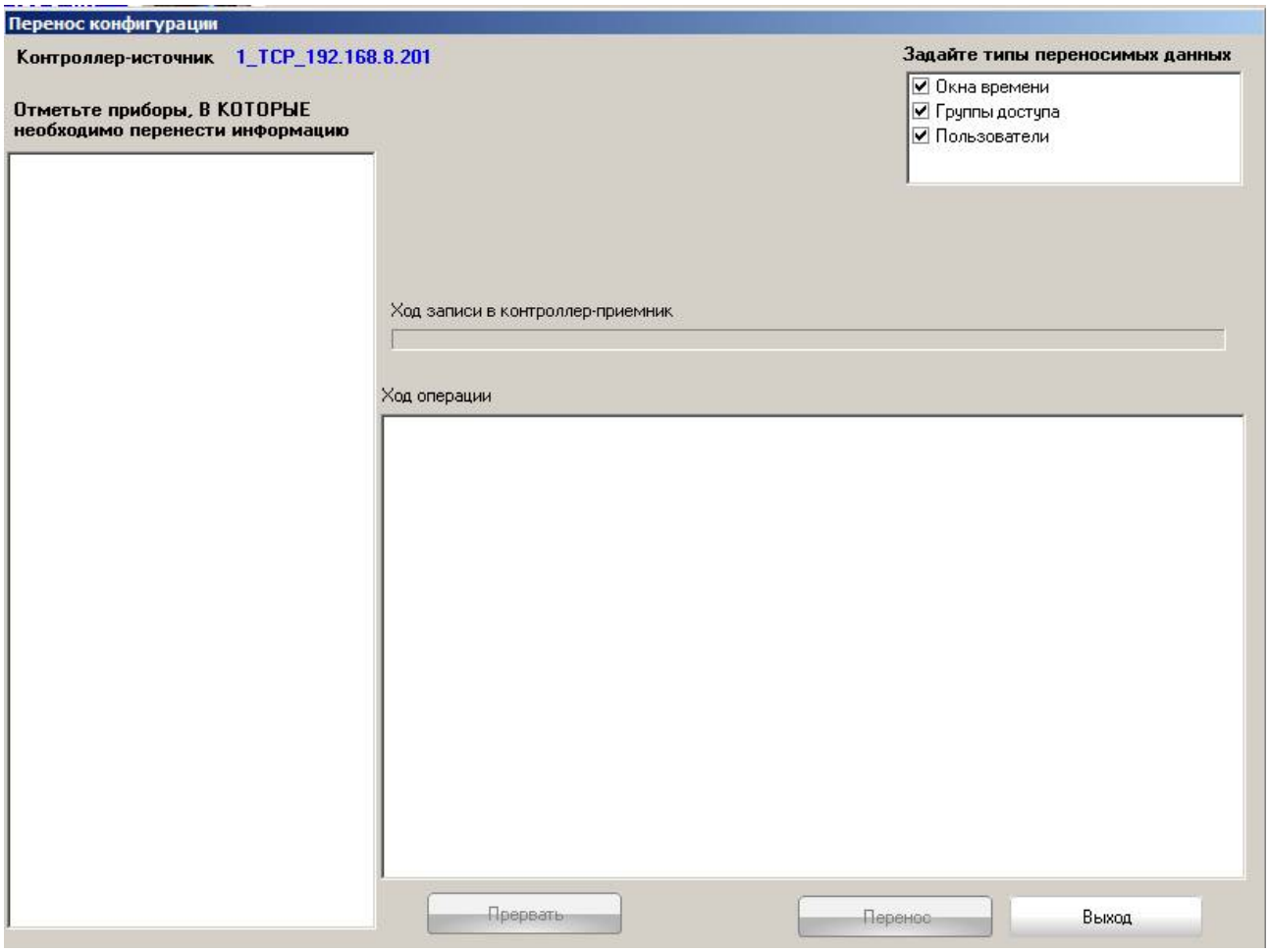


Рисунок 47

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».

Вкладка «Руководство»

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

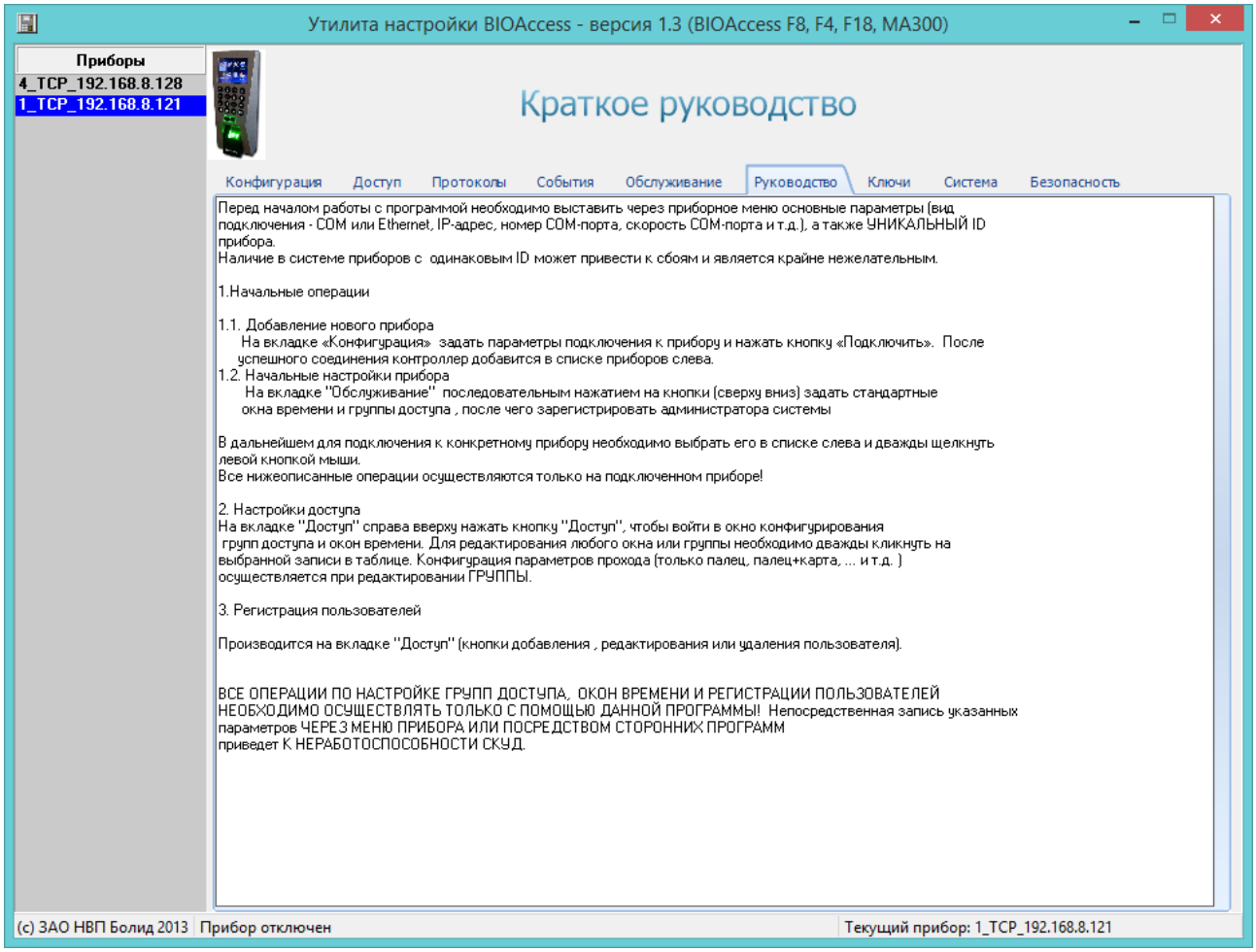


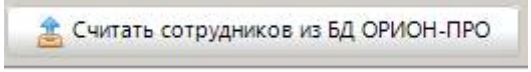
Рисунок 48

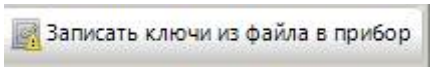
Вкладка «Ключи»

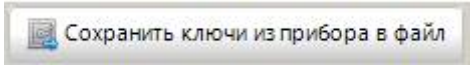
На этой вкладке осуществляется экспорт ключей из контроллера в базу данных «Орион Про».

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.

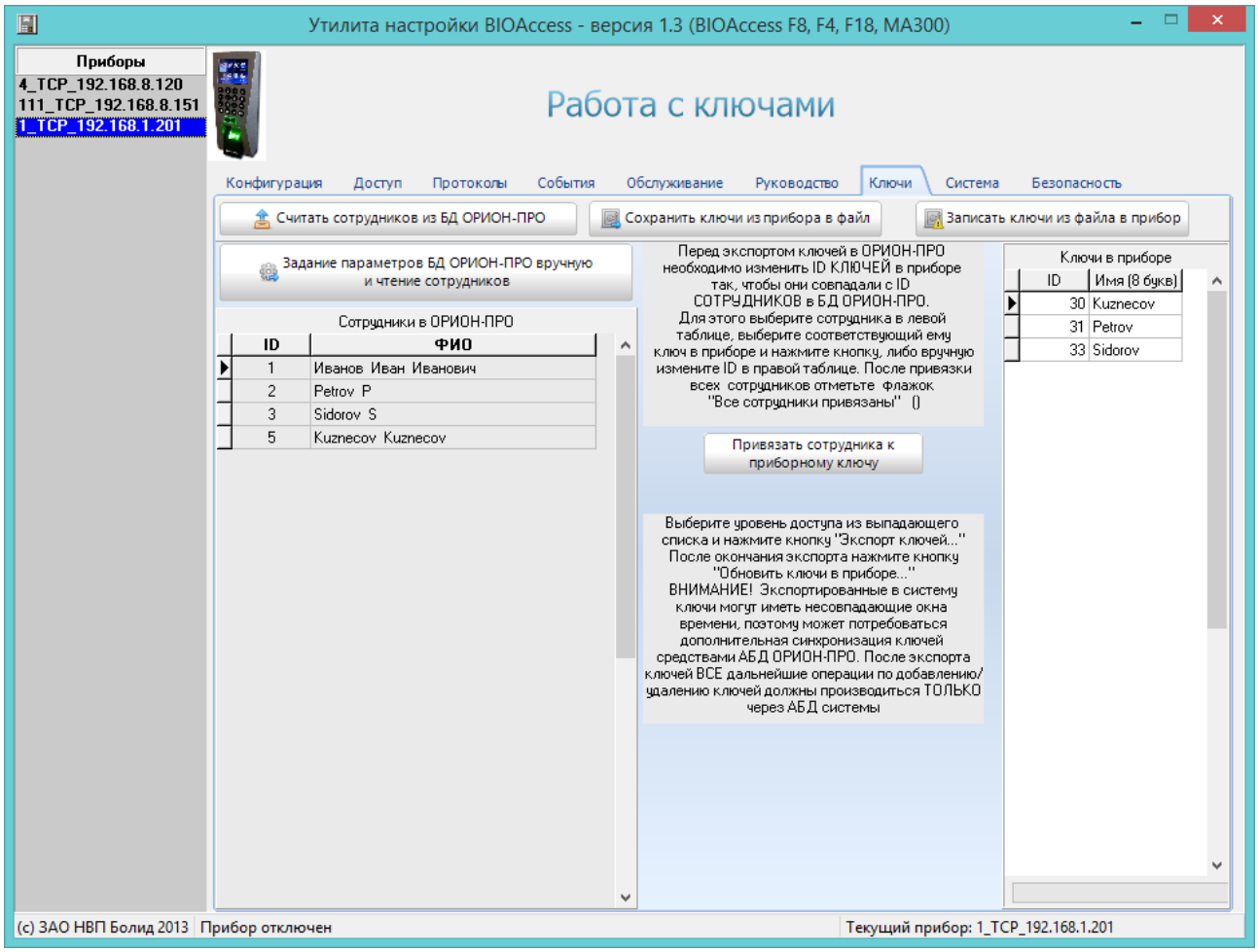
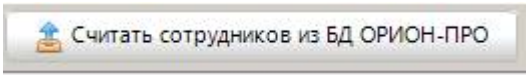
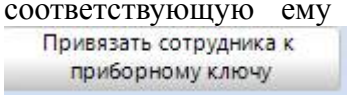


Рисунок 49

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

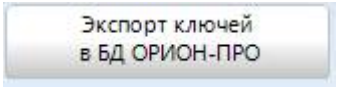
В левом столбце после нажатия на кнопку 

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

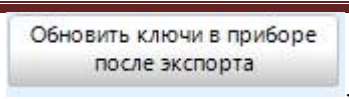
Перед экспортом ключей в «Орион Про» необходимо изменить номера (ID) ключей в контроллере так, чтобы они совпадали с ID сотрудников в базе данных «Орион Про». Для этого нужно выбрать сотрудника в списке «Сотрудники в ОРИОН-ПРО», выбрать соответствующую ему запись в списке «Ключи в приборе» и нажать на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

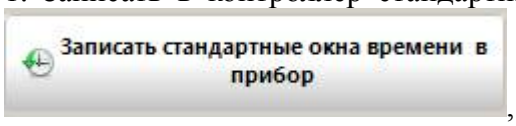
на кнопку 

.

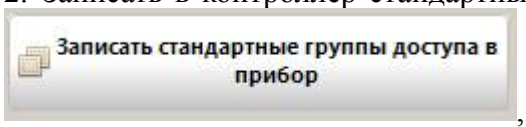
Экспортированные в систему ключи могут иметь несовпадающие окна времени, поэтому может потребоваться дополнительная синхронизация ключей средствами Администратора Базы Данных «Орион Про».

Начальная настройка контроллера

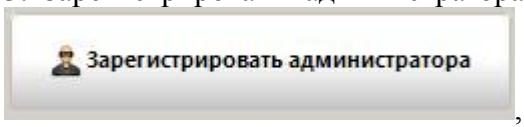
Для того чтобы контроллер можно было использовать в ИСО «Орион Про», необходимо на вкладке «Обслуживание» программы BAProg выполнить следующие операции:

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»

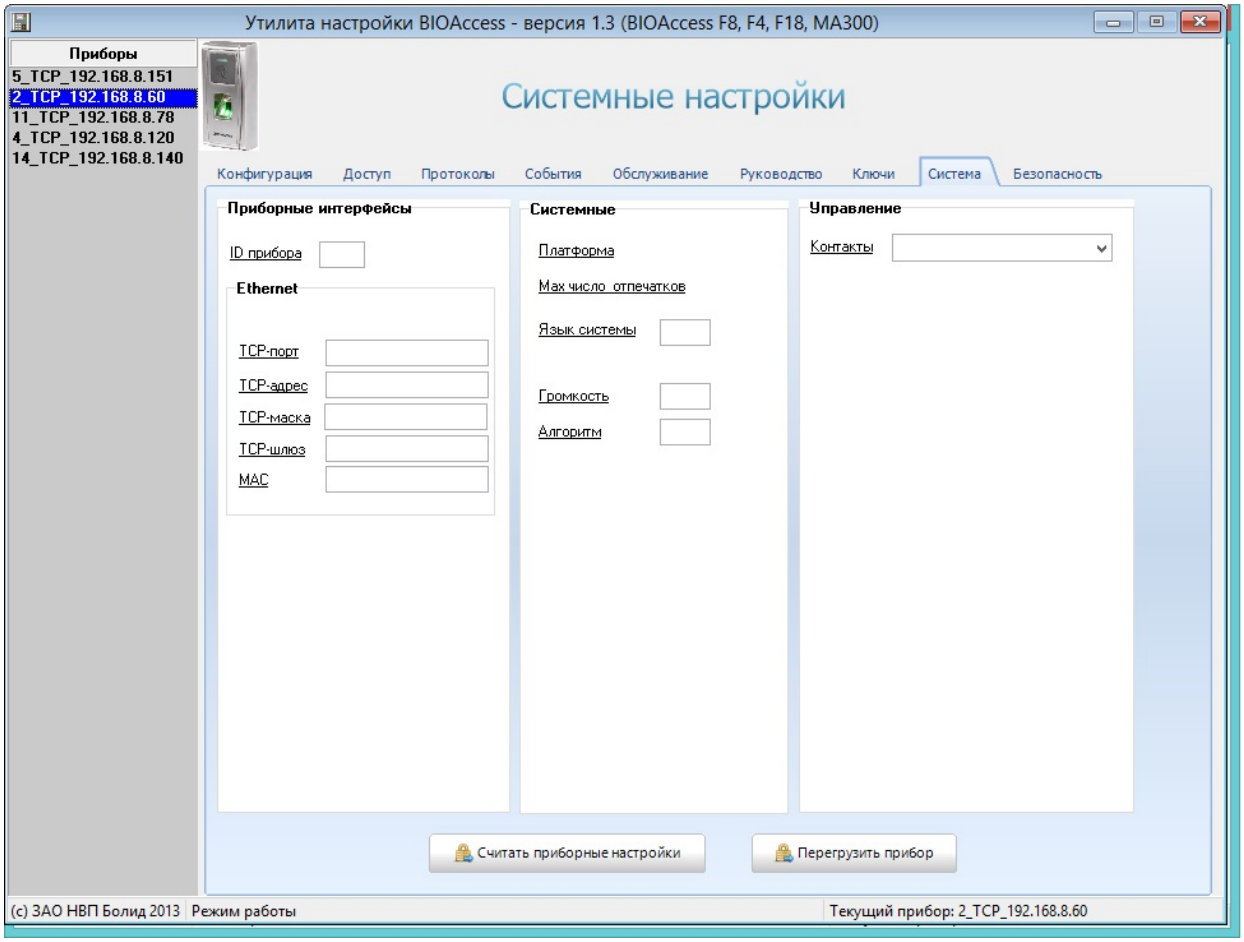


Рисунок 50

Вкладка «Безопасность»

Данная вкладка предназначена для задания параметров защищенного режима (ЗР). Этот режим реализован только в контроллерах С2000-BIOAccess -МА-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 С2000-2, 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 С2000-2 зарегистрировать пользователя с данным ключом доступа (код ЭТОЙ ЖЕ "секретной" карты), и дать ему полномочия на проход.

ВАЖНО! В биометрическом контроллере и в контроллере 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.)

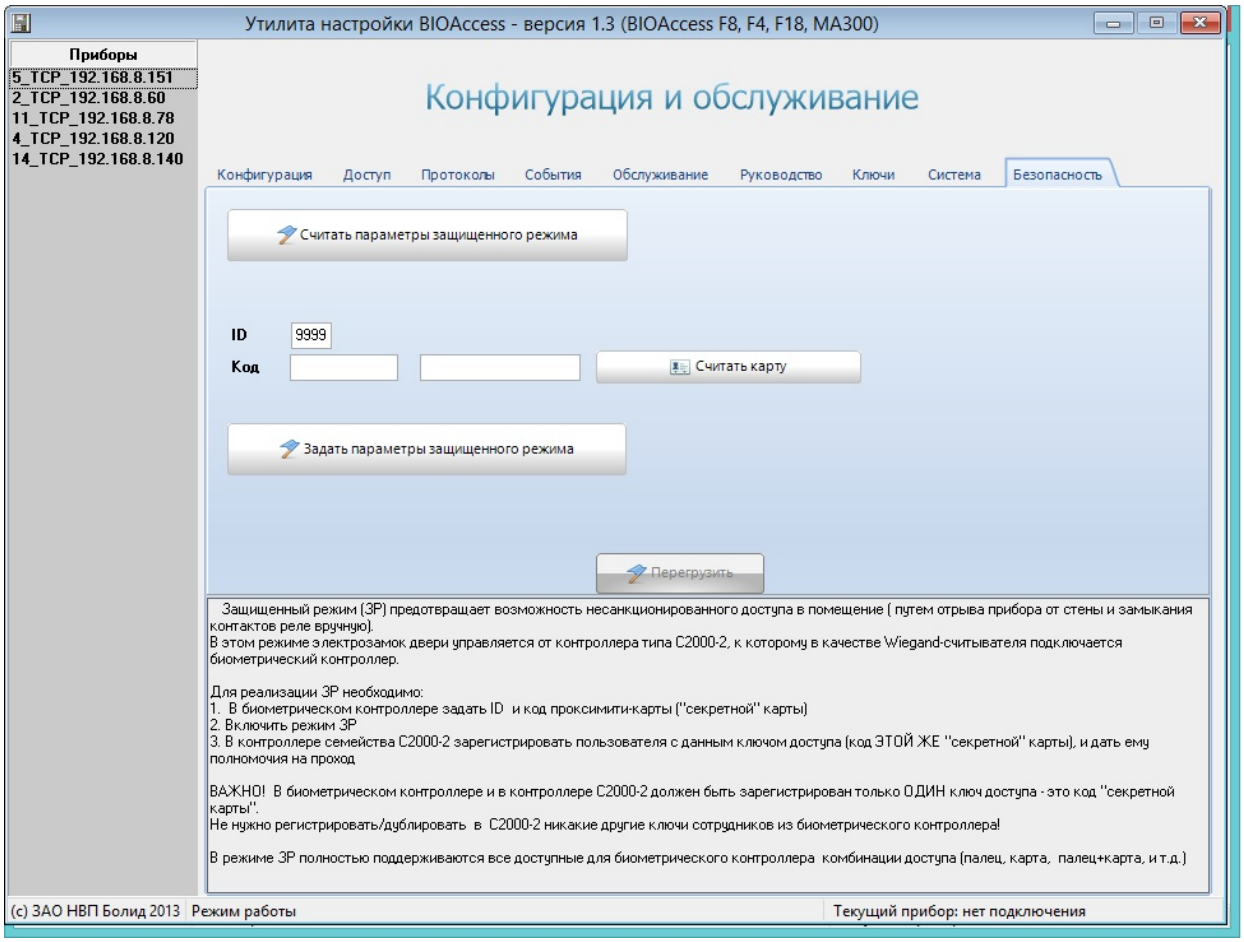


Рисунок 51

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.

Настройка контроллера в BAProg

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

- **Клавиатура и дисплей** – очистка при появлении видимых загрязнений и затруднении чтения.
- **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-BIOAccess-F18» соответствует требованиям технического регламента Таможенного союза ТР ТС 020/2011. Имеет сертификат соответствия № RU C-RU.ME61.B.00445