ПАСПОРТ

Универсальный автономный считыватель-контроллер «Привратник-03А»

Настоящий паспорт удостоверяет гарантированные изготовителем основные параметры и характеристики универсального считывателя-контроллера **Привратник-03А**.

Общие сведения об изделии.

Универсальный считыватель-контроллер **Привратник-03А** предназначен для применения в автономных системах контроля доступа в помещения банкомата. В качестве карт доступа в помещение считывателем-контроллером принимаются любые банковские карты всех платежных систем как с магнитной полосой (согласно ISO 7813), так и с микропроцессором (согласно ISO 7816).

Конструктивное исполнение универсального считывателя-контроллера позволяет использование его как во «врезном» варианте, так и в накладном (через специальный бокс-корпус).

Технические характеристики устройства.

1	Напряжение питания, В	12±10%
2	Ток потребления устройства, mA*	не более 100
3	Ток нагрузки на выходе устройства, А	не более 2
4	Время подачи импульса на замок, сек.	от 1 (программируется)
5	Температурный диапазон работы, °С	от –30° до +35°

* - без учета тока потребления замка\защелки

Комплектация изделия

1	Считыватель-контроллер	1 шт.
2	Комплект крепежа (антивандального)	1 шт.
3	Панель передняя антивандальная	1 шт.
4	Кнопка выхода, накладная	1 шт.
5	Наклейки информационные	1 комплект
6	Паспорт на изделие	1 шт.
Компоненты, поставляемые опционально		
7	Бокс для накладного варианта установки	1 шт.
8	Считыватель бесконтактных карт NFC	1 шт.
9	Датчик обнаружения скимминга	1 шт.

Особенности монтажа универсального считывателя-контроллера Привратник-03А

Конструктивно универсальный считыватель пластиковых карт выполнен как устройство для врезной (скрытой) установки. Устройство монтируется на поверхности, граничащей с блокируемым дверным проходом. Крепление к поверхности осуществляется через специальные монтажные отверстия, расположенные на лицевой передней антивандальной панели считывателя. Внешний вид считывателя-контроллера в сборе представлен на **рис.1**. В случаях, когда дверной блок обрамлен металлостеклянными витражами, возможна установка считывателя-контроллера в специальный накладной бокс. Данный бокс является опциональной позицией и заказывается отдельно.

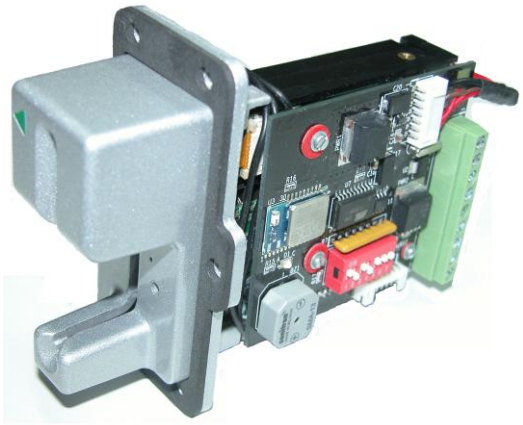

рис.1

Описание работы универсального считывателя-контроллера Привратник-03А

Устройство «Привратник-03А» содержит в своем составе универсальный считыватель пластиковых карт и контроллер. Контроллер принимает и обрабатывает данные, поступающие со считывателя карт, с внешних датчиков (кнопка выхода, блокировка, датчик присутствия) и управляет работой блокирующего устройства двери (электромагнитный замок, электромеханическая защелка).

При подаче питающего напряжения (+12 В постоянного тока) устройство переводится в ждущий режим. В зависимости от начальных настроек с привязкой к времени суток дверь переходит в режим блокировки (замком, защелкой) или остается разблокированной (свободный проход). В случае если дверь по состоянию настройки остается разблокированной – цвет светодиода, расположенного на передней панели считывателя остается «зеленым». Если дверь блокируется – светодиод переходит в режим переменного мигания зеленым и красным цветом.

При установке в считыватель карты установленного образца и разрешенная к проходу - дверь разблокируется на время, определенное настройками контроллера, раздается звуковой сигнал оповещения о разрешении прохода, индикация светодиода меняется на постоянный зеленый. Отсчет времени разблокировки двери ведется с момента извлечения банковской карты из считывателя пользователем. По истечении данного временного интервала дверь блокируется, и устройство переводится в ждущий режим. Разблокировка двери изнутри помещения производится нажатием кнопки выхода, подключенной к контроллеру.

Устройство позволяет реализовать ряд дополнительных функций, расширяющих возможности работы системы:

А) полная блокировка входной двери – на случай инкассации банкомата или блокировки помещения в случае проведения видимых спорных транзакций или проявления актов вандализма. Данная блокировка обеспечивается подключением концевого выключателя с фиксацией (тумблера) или контактов реле видеорегистратора к соответствующим выводам контроллера. При активации данного режима система не реагирует ни на кнопку выхода и не считывает карты.

Б) блокировка входной двери на вход – данная функция препятствует проходу в помещение банкомата в случае, если там уже находится и обслуживается держатель карты. Реализация данной функции осуществляется подключением охранного шлейфа объемного датчика, установленного у банкомата.

В) обнаружение нештатных внешних устройств – данная опциональная функция позволяет обнаруживать скимминговые накладки на считыватель системы. При срабатывании соответствующего датчика дверь разблокируется, одновременно световая и звуковая индикация переводится в соответствующий режим. На определенном контакте клеммника (**Е**) появляется управляющее напряжение, позволяющее реализовать соответствующие обстановке (режиму) устройства и алгоритмы.

На передней панели считывателя имеется сервисное отверстие, позволяющее экстренно извлечь застрявшую пластиковую карту (к примеру, установленную в выключенный считыватель). Для этого потребуется либо игла, либо фрагмент канцелярской скрепки.

Описание компонентов платы универсального считывателя-контроллера Привратник-03А

Плата контроллера изделия содержит в своем составе ряд коммутационных элементов, которые используются в работе устройства и задействуются при монтаже изделия.

Расположение разъемов на плате контроллера приведено на **рис.2**.Подключение внешних линий питания и управления к контроллеру осуществляется посредством клеммника **Х3**.

Плата содержит также разъем интерфейсного соединения **Х4** (для связи со считывателем изделия). Разъем **Х1**, расположенный на обратной стороне платы контроллера, является сервисным и в работе не используется. Разъем **Х5** предназначен для подключения опционального считывателя бесконтактных банковских карт, а также для датчика обнаружения скимминговых накладок на считыватель устройства.

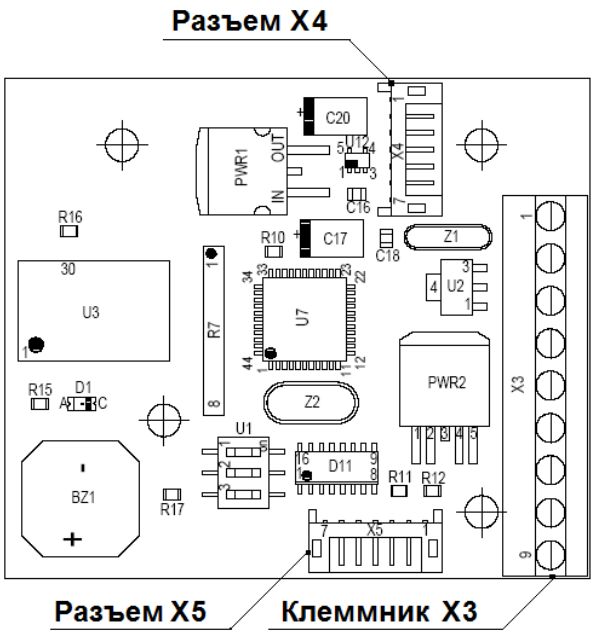

рис.2

Подключение универсального считывателя-контроллера Привратник-03А

Контроллер изначально запрограммирован и готов к работе. Окна настроек заполнены типовыми значениями переменных и констант, которые контроллер использует в своей работе. Подключение внешних линий питания и управления к контроллеру осуществляется посредством клеммника **X3**, назначение контактов которого приведено на **рис.3**.

G	GND
+	+12 В
R	Антискимминг (вход)
E	Антискимминг (выход)
D	Управление замком
C	Датчик присутствия
B	Блокировка
A	Кнопка выхода
G	GND

рис.3

Типовая схема подключения считывателя-контроллера показана на **рис.4**. На схеме также приведены наименования внешних коммутационных устройств (обмотка э/магнитного замка, кнопка выхода, блокировка (с фиксацией) и НЗ контакты датчика присутствия). Также в качестве внешних цепей указаны датчик обнаружения скимминговой накладки и устройство отрабатывающее алгоритм работы по факту обнаружения нештатного внешнего устройства.

Защита от скимминговой атаки является опциональной и по умолчанию программно отключена. Также программно отключен сервис контроля за датчиком присутствия клиента.

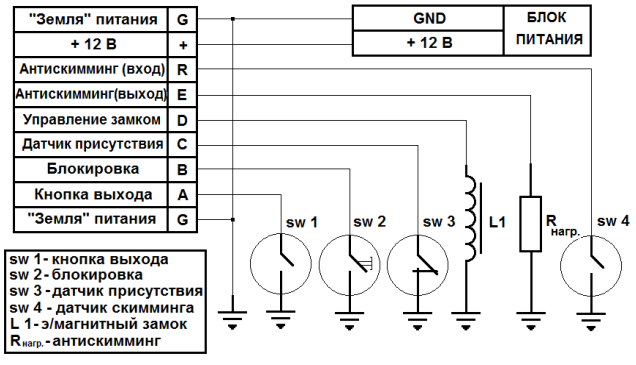

рис.4

Работа с универсальным
считывателем-контроллером Привратник-03А

Контроллер изначально запрограммирован и готов к работе. После включения устройства в зависимости от времени суток устройство переводится в 2 разных варианта ждущего режима. В случае, если включение контроллера произошло в интервале с 20-00 до 8-00 (МСК) дверь переходит в режим блокировки, светодиод переходит в режим переменного мигания зеленым и красным цветом. В случае если включение произошло в другом временном диапазоне - дверь остается разблокированной – цвет светодиода, расположенного на передней панели считывателя остается «темным».

Для осуществления изменения настроек, синхронизации с местным временем, а также при необходимости организовать просмотр и выгрузки логов по проходам - необходимо установить на мобильном устройстве бесплатное программное обеспечение **PRIVRATNIK 03**. Для установки приложения необходимо убедиться в поддержке смартфоном:

- установленной версии ANDROID OS не ниже 4.3;
- Bluetooth 4.0, включая поддержку низкого энергопотребления (англ. Bluetooth Low Energy, Bluetooth LE);

Далее, по QR-коду на последней странице Руководства необходимо скачать файл Privratnik.apk и установить Приложение. После установки приложения на рабочем столе появится ярлык (**рис.5**):

Рис.5

В основном меню устройства следует активировать беспроводной интерфейс связи BLUETOOTH для соединения со считывателем-контроллером «Привратник-03А». После запуска приложения на смартфоне появится сервисное окно поиска устройства (**Рис.6**). После обнаружения устройства в появившемся меню необходимо выбрать окно с наименованием обнаруженного устройства BLUEGIGA PRIVRATNIK (**Рис.7**):

Рис.6

Рис.7

После чего появится окно с указанием данных о неизвестном устройстве, которое следует выбрать (**Рис.8**),

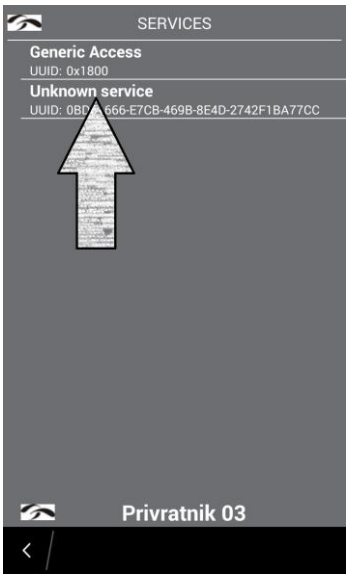

Рис.8

далее следует выбрать появившийся вариант устройства (**Рис.9**)

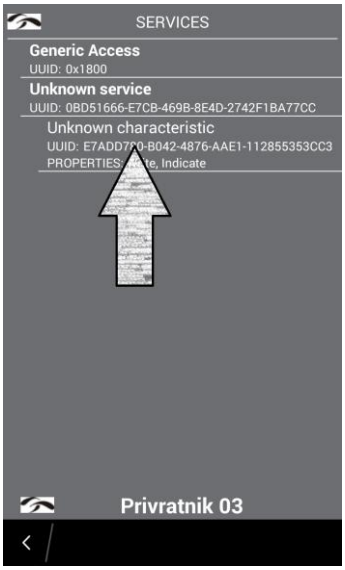

Рис.9

После действий описанных выше на экране появится меню программы PRIVRATNIK 03 (**Рис.10**). После чего следует выгрузить в окна меню актуальные настройки для контроллера

(по умолчанию). Для этого необходимо нажать на пиктограмму выгрузки - символ в правом верхнем углу меню.

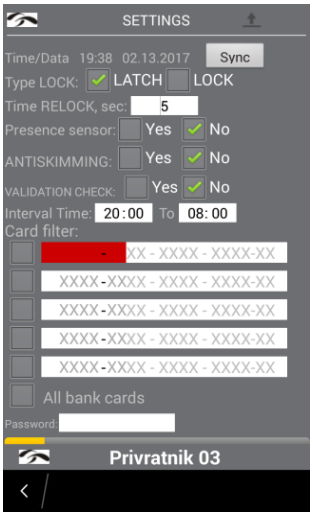

Рис.10

В случае Ваших корректных действий внизу появится бегущая шкала желтого цвета, сигнализирующая о ходе выполнения Вашего запроса. После выполнения запроса окна меню заполнятся актуальными для контроллера настройками. (**Рис.11**)

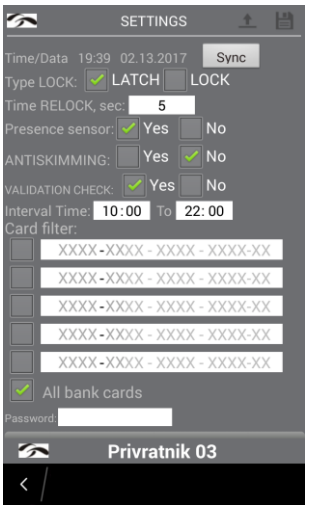

Рис.11

Описание окон меню приложения PRIVRATNIK 03

На **рис.12** приведен скриншот экрана основного меню приложения.

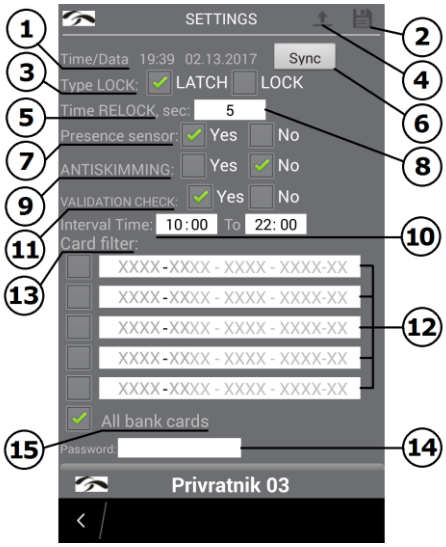

Рис.12

1	Текущее системное время смартфона
3	Тип блокирующего устройства (замок/защелка)
5	Время открытия замка
7	Выбор датчика присутствия
9	Выбор датчика обнаружения скимминга
11	Выбор проверки карт на срок действия
13	Раздел фильтров карт
15	Выбор прохода всех типов карт

2	Загрузка настроек в контроллер
4	Выгрузка настроек из контроллера
6	Синхронизация времени
8	Окно ввода времени открытия замка
10	Окна ввода времени работы контроллера
12	Окна ввода номеров карт
14	Окно ввода пароля для входа в меню логов

Пояснения:

1 и **6** – в случае если местное время **отличается от московского**, **необходимо** провести синхронизацию системного времени смартфона с контроллером;

4 и **2** – пиктограммы используются для выгрузки настроек контроллера на смартфон и последующей загрузки измененных настроек на устройство.

3 – выбор типа блокирующего устройства определяется вариантом, который используется в конкретном случае – э/магнитный замок или э/механическая защелка;

5 и **8** – данная настройка определяет временной интервал в течении которого будет открыта дверь при открытии ее картой или кнопкой выхода, в соответствующее окно необходимо вести величину в секундах;

7 – в данной настройке выбирается, будет или не будет использоваться в системе датчик присутствия клиента в зоне банкомата;

9 - в данной настройке выбирается, будет или не будет использоваться в системе датчик обнаружения скимминговых накладок на считыватель системы;

Примечание – если в системе указанные датчики использоваться не будут – обязательно поставьте галки в окнах NO. В противном случае контроллер будет выдавать соответствующие звуковые и световые сигналы !

10 – в данные окна заносится время начала и окончания работы системы для осуществления прохода по картам;

11 - в данной настройке активируется или отключается режим отслеживания сроков действия карт, предъявляемых к проходу;

12 – в указанные поля заносятся старшие 6 символов номеров банковских карт, если будет использоваться фильтр карт;

13 – раздел активации фильтра карт. Устройство поддерживает 5 разных масок по старшим 6 символам номера банковской карты. Для активации фильтра необходимо поставить галку в соответствующее поле и заполнить фильтр необходимыми цифрами;

14 – поле ввода пароля для доступа в меню логов контроллера;

15 – сброс фильтра карт, активация режима пропуска всех банковских карт (любого банка, любой платежной системы);

Особенности использования внешних датчиков

Кроме кнопки выхода к устройству можно подключать несколько внешних датчиков (цепей):

1. Датчик присутствия клиента.
2. Внешняя блокировка системы.
3. Датчик обнаружения скимминговой накладки.

В качестве Датчика присутствия рекомендуется использовать объемный ИК-датчик, направленный на рабочую зону у банкомата. При наличии посетителя внутри сервисной зоны банкомата система не позволит открыть снаружи дверь картой. Об активации указанного режима будет свидетельствовать световая и звуковая индикация. При этом кнопка выхода будет работать, позволяя клиенту беспрепятственно покинуть помещение банкомата.

Внешняя блокировка предназначена для полной блокировки входной двери в зону банкомата. Может осуществляться как внешним переключателем, так и релейными выходами контрольных панелей охранной сигнализации или видеорегистраторов. Функция актуальна для блокировки двери при осуществлении инкассации банкомата или при обнаружении признаков мошеннических действий посторонними лицами у банкоматов.

Датчик обнаружения скимминговой накладки фиксирует появление нештатных устройств и конструкций поверх панели считывателя. При обнаружении подобных устройств контроллер блокирует дверь на вход, переходит в режим тревоги и выдает на выход **E** уровень +12В. К выходу можно подключить световые (звуковые) оповещатели с током потребления не более 0,7 А. При этом кнопка выхода будет работать, позволяя клиенту беспрепятственно покинуть помещение банкомата.

На **рис.4** приведена условная схема подключения всех возможных внешних цепей (датчиков и исполнительных устройств).

Работа с фильтрами карт

Системное программное обеспечение контроллера позволяет организовать 5 разных масок для реализации фильтра по номерам банковских карт, предъявляемых к проходу.

Наличие данного функционала позволяет ограничить доступ к банкомату карт, как по типу платежной системы, так и по банку эмитенту карты.

Функция бывает полезной, когда собственник банкомата хочет ограничить перечень обслуживаемых лиц только кругом своих клиентов (в рамках программ лояльности, зарплатного проекта и т.д.).

Для начала работы с фильтрами карт достаточно коснуться экрана в месте установки галки напротив поля заполнения старших символов номера банковской карты. После установки галки поле ввода номера подсветится красным цветом и будет готово к вводу символов.

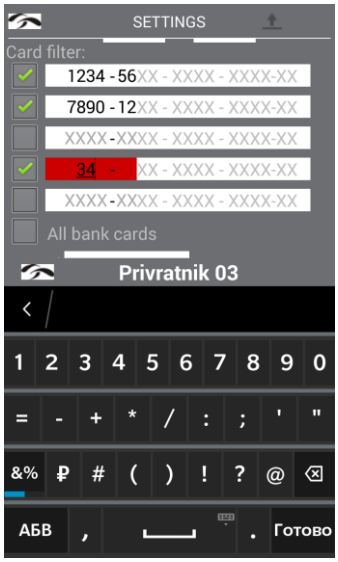

Рис.13

После ввода старших символов номеров карт достаточно коснуться пальцем в любой свободной области экрана. Красная область заполнения исчезнет, далее следует прогрузить настройками контроллер (флоппи в правом верхнем углу экрана). Теперь контроллер при считывании номеров карт будет их сверять с введенными масками и разрешать (или не разрешать) проход в помещение банкомата.

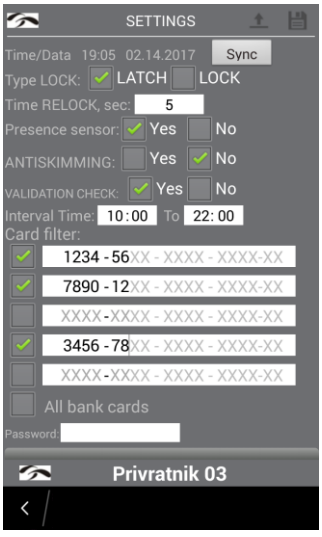

Рис.14

Работа с лог-файлом контроллера

Контроллер способен сохранять лог-файл по проходам. Информация лога содержит: номер карты, время прохода и реакция системы на попытку прохода.

Работа с лог-файлом возможна как на смартфоне – путем просмотра таблицы данных с кодами событий. Также возможна выгрузка лог-файла на смартфон – для дальнейшей работы с таблицей данных. В этом случае коды событий уже замещаются описанием (на английском языке) самих событий, как например:

- *Успешный проход;*
- *Карта запрещена к проходу;*
- *Истек срок действия карты;*
- *Помещение занято клиентом;*

Для доступа к лог-файлу через приложение необходимо наличие пароля. Данный пароль (ПИНКОД) является уникальным для каждого контроллера и устанавливается при производстве. Указанный пароль выдается при продаже контроллера и приводится на финальном оборотном листе данного Руководства.

Для ввода пароля достаточно перейти в окно ввода ПИНКОДа – **рис.16**

Рис.16

Затем необходимо полностью ввести пароль. После чего следует прогрузить настройками контроллер (флоппи в правом верхнем углу экрана).

После корректного ввода пароля и прогрузки контроллера на экране меню появится активная кнопка Logs (**рис.17**).

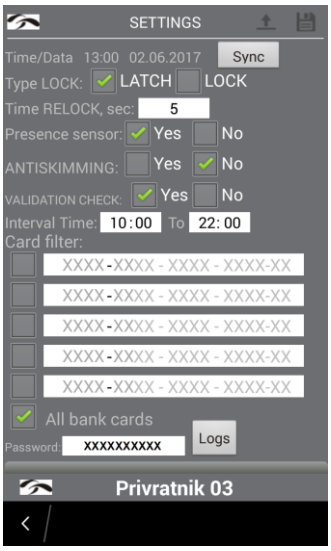

Рис.17

При нажатии на кнопку **Logs** приложение переходит в экран работы с лог-файлом (**рис.18**).

Рис.18

При нажатии на кнопку **Read Logs** стартует выгрузка данных на экран приложения, которые представлены в виде таблицы **рис.19**. Указанные данные можно просмотреть, а также пользователю доступна выгрузка на мобильное устройство путем нажатия на кнопку **Save.**

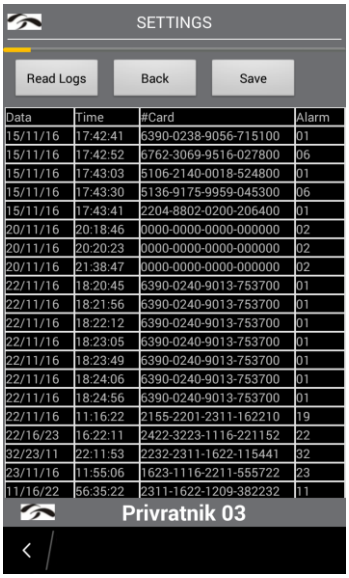

Рис.19

Результатом выгрузки будет файл **LogFile.csv**, который Приложение разместит на смартфоне в директории **Download.** Данный файл является табличным. При просмотре в любом табличном редакторе данные представляются в виде как в **Табл.1**

Табл.1

"Data"	Time	#Card	Alarm
15/11/16"	17:42:41	6290-0732-9056-715100	Successfully.
15/11/16"	17:42:52	6762-9769-3416-027800	Card prohibited.
15/11/16"	17:43:03	5206-2243-0018-524800	Successfully.
23/11/16"	12:09:32	2304-7602-0200-206400	Successfully.
23/11/16"	12:50:54	5481-7325-0154-991900	Card prohibited. Validity of the card has expired.
23/11/16"	13:05:21	2104-8102-0220-640022	Successfully.

Для возврата в основное меню достаточно нажать кнопку **Back**. Приложение откроется основным экраном без актуальных параметров настроек (**рис.20**). После чего следует

выгрузить в окна меню актуальные настройки для контроллера. Для этого необходимо нажать на пиктограмму выгрузки - символ в правом верхнем углу меню.

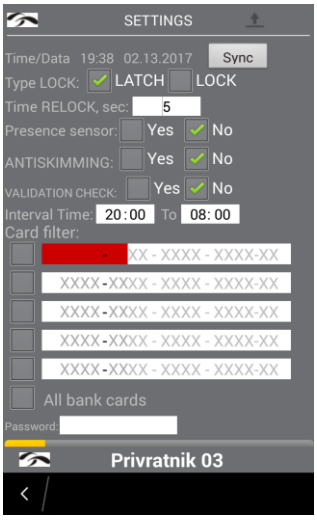

Рис.20

После выполнения запроса окна меню заполнятся актуальными для контроллера настройками. (**Рис.21**)

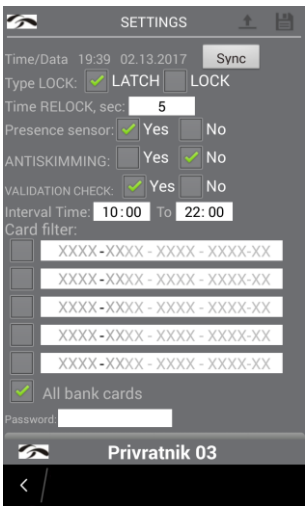

Рис.21

Сервисные OBD функции универсального считывателя-контроллера Привратник-03А

Отличительной особенностью контроллера является встроенная диагностика состояния оборудования системы контроля доступа – таких как целостность линий питания и управления внешних устройств (э/магнитный замок, кнопка выхода), диагностируется также состояние и самого контроллера.

Данный сервис построен по принципу OBD, таблица блинк-кодов и звукового оповещения состояний оборудования приведена ниже:

Табл.2

	Состояние системы, ошибки	**Свечение светодиода**			**Звуковой излучатель**
		Зеленый	**Красный**	**Желтый**	
режимы	Свободный проход	постоянно			
	Режим ожидания	мигает	мигает		
	Вход разрешен	постоянно			постоянно
	Карта запрещена[1]		мигает		с интервалом
	Обнаружен скимминг	мигает	мигает	мигает	с интервалом
	Клиент внутри			постоянно	
	Блокировка[2]		мигает		с интервалом
ошибки	Ошибка кнопки[3]	мигает	мигает		постоянно
	Обрыв нагрузки		мигает	мигает	
	Карта не извлечена		мигает		с интервалом
	Ошибка связи	не светит	не светит	не светит	с интервалом

Примечание:

1. В случае если в считыватель установлена карта не соответствующая формату разрешенной, проход по ней не разрешён о чем короткими (0,3 сек.) импульсами сигнализируют излучатели звуковой и световой индикации.
2. В случае активации режима Блокировки звуковая и световая индикация следуют с импульсами 0,5-1 сек.
3. В случае если Кнопка выхода продавлена, устройство переходит в аварийный режим, при котором дверь разблокируется. Светодиод зеленого цвета переходит в режим постоянного излучения.

Дополнения:

Ошибка связи контроллера устройства с модулем считывателя требует вмешательства на аппаратном уровне. Все остальные ошибки сбрасываются автоматически при устранении причины их возникновения.