



Прибор охранной сигнализации
ТСИ-03
«SlyGuard»

Руководство пользователя
Rev. 2.7



СОДЕРЖАНИЕ

Назначение изделия.....	4
1. Основные функции и характеристика работы устройства.....	4
2. Отличительные особенности системы.....	4
3. Основные понятия и определения.....	7
4. Режимы работы устройства.....	9
4.1. Режим «Снят с охраны».....	9
4.2. Режим «Охрана».....	9
4.3. Состояние «Тревога».....	10
5. Работа с SMS-сообщениями.....	11
5.2. Структура SMS сообщений.....	12
5.3. SMS команды.....	13
6. Настройка параметров работы устройства.....	15
6.2. Работа с радиобрелками.....	16
6.2.1. Изменение режима работы радиомодуля.....	16
6.2.2. Процедура обучения радиобрелков.....	16
6.3. Работа с электронными ключами и картами доступа.....	18
6.3.1. Изменение режима работы модуля электронных ключей.....	18
6.3.2. Процедура изменения MasterKey.....	19
6.3.3.Процедура изменения базы кодов-идентификаторов электронных ключей..	19
6.4. Сервисная программа для настройки параметров терминала.....	21
6.4.1. Меню сервисной программы.	23
6.4.2. Объект настройки «Клиенты».....	24
6.4.3. Общие настройки.....	26
6.4.4. Закладка «Видео».....	27
6.4.5. Объект настройки «Параметры терминала».....	29
6.4.6. Объект настройки «Цифровые входы».....	30
6.4.7. Объект настройки «Аналоговые входы».....	32
6.4.8. Объект настройки «Выходы терминала».....	34
6.4.9. Объект настройки «Параметры Связи».....	36
6.4.10. Объект настройки «Управление Доступом».....	38
7. Подключение устройства.....	40
7.1. Назначение выводов разъема.....	40
7.2. Общая схема подключения.....	41
7.3. Подключение Питания терминала ТСИ-03.....	44



7.4. Подключение GSM-антенны.....	45
8. Внешний вид устройства.....	45
9. Внешний вид и подключение элементов расширения.....	46
10. Основные технические характеристики.....	47
Приложение А. Пояснения к тексту.....	49
Приложение Б. Специфические схемы подключения устройства.....	51
Б.1. Защищенное подключение устройств с контактным выходом к цифровым входам устройства.....	51
Б.2. Принцип действия подключения.....	51
Б.3. Подключение датчиков с контактным выходом к аналоговым входам устройства.....	52
Приложение С. Процедура работы двух (основной и резервной) SIM-карт.....	54
Приложение Д. Извещения от встроенных индикаторов.....	55



Назначение изделия

Терминал стационарный интегрированный ТСИ-03 предназначен для работы в качестве информирующего устройства в составе комплекса диспетчеризации, мониторинга и охраны жилых и нежилых стационарных объектов, например складов, домов, дач, гаражей и т.п. Данное устройство объединяет в себе систему удаленного управления и автоматизации, прибор приемо-контрольный¹. Устройство рассчитано на работу в сети сотовой связи стандарта GSM и поддерживает передачу данных в SMS сообщениях и посредством GPRS-канала.

Получателями информации, поступающей от терминала, могут быть как конечные пользователи (владельцы), так и централизованные диспетчерские центры, обеспечивающие круглосуточный контроль состояния охраняемого объекта и осуществляющие в случае необходимости экстренное оперативное реагирование.

Терминал ТСИ-03 также может быть использован в качестве масштабируемой системы контроля и управления доступом, а также системы дистанционных измерений параметров технологических процессов и управления ими.

1. Основные функции и характеристика работы устройства

К терминалу подключаются любые датчики² или законченные системы³ (устройства) с контактным выходом, что позволяет без особых усилий интегрировать терминал в уже установленные на объектах охранные комплексы. Для интеграции с терминалом устройств с различными параметрами выходного (тревожного) сигнала⁴ предусмотрены цифровые⁵ (8 «сухих контактов») и аналоговые входы⁶ (4 шлейфа) с индивидуальной настройкой алгоритма регистрации тревожных событий.

С помощью имеющихся 4-х перекидных реле⁷ (2 в терминале + 2 на монтажной плате, управляемых схемой с открытым коллектором терминала), возможно автоматическое или дистанционное управление подключенными исполнительными устройствами⁸.

Одной из особенностей данного терминала является его функционирование в качестве устройства контроля и управления доступом на охраняемый объект. Ограничение доступа осуществляется с помощью радиобрелока (2 шт. в комплекте поставки) и контроллера TouchMemory/iButton. В памяти устройства хранится до 128 ключей доступа. С помощью программы настройки терминала есть возможность гибкой настройки его действий при активации того или иного ключа или брелока.

Расположенные на корпусе терминала индикаторы показывают его текущее состояние (нормальное/аварийное/тревожное состояние, выполнение служебных процедур, контроль GSM сигнала и т.п.).

2. Отличительные особенности системы

Общие характеристики:

- 8 входов для подключения групп датчиков типа «сухой контакт».
- 4 входа для подключения датчиков, передающих данные в аналоговом формате (изменение напряжения).
- 2 перекидных реле и 2 Открытых Коллектора (управляют 2-мя перекидными реле на Монтажной Плате - опционально).
- 8 телефонных номеров клиентов в «Телефонной книге» SIM-карты или в профиле терминала.



- Встроенный интерфейс RS-232 для подключения периферийных устройств различного назначения.
- Разъем для подключения активных микрофонов для удаленной прослушки контролируемого объекта.
- Встроенный модуль работы с радиобрелками (частота 433 МГц) и модуль iButton/TouchMemory.
- Информативная светодиодная индикация на компактном, ударопрочном и эстетичном корпусе устройства.
- Удобная выносная монтажная плата для стандартных стальных боксов.
- Работа с двумя SIM-картами различных операторов.

Каналы связи и управление работой:

- Передача извещений от терминала по каналам GSM, SMS, GPRS.
- Управление состояниями терминала посредством SMS и GPRS команд, радиобрелоков, электронных ключей и карт.
- Широкие полномочия по удаленному администрированию терминала одним привилегированным клиентом (администратор) – Дистанционные смена телефонных номеров клиентов, блокирование доступа радиобрелков или электронных ключей.

Настройка и конфигурирование:

- Возможность упрощенной настройки терминала для полноценного функционирования с помощью телефона владельца, без подключения ПК.
- Дружественный интерфейс и информативность программы конфигурирования терминала (подключение к ПК через mini-USB интерфейс).
- Гибкая настройка параметров «сухих контактов» входов (нормально замкнутый / нормально разомкнутый / импульс; «активен на охране» / «активен всегда»).
- Автоматическая настройка тревожных значений на подключаемых к аналоговым шлейфам устройствах измерения и сигнализации, либо ручной ввод этих значений из паспорта этих устройств.
- Гибкая настройка выполняемых действий на 4-х релейных выходах (замкнуть/разомкнуть/последовательность переключений заданной длительности).
- Возможность задания удобных для чтения на телефоне пользователя имен-псевдонимов входов и выходов терминала.
- Возможность перезаписи Мастер Ключа на объекте при его утере.

Особенности функционирования:

- Возможность обработки информации от любых типов современных охранных датчиков.
- Самотестирование устройства и подключенных шлейфов при постановке на охрану.
- Автоматическая активация заданных выходов при возникновении определенных событий на конкретных входах.
- Коммутируемая нагрузка реле до 3 А на канал (суммарно не более 12А).
- Передача текущих значений (в у.е.) на аналоговых входах при достижении тревожных значений или по запросу.



- Передача администратору идентификаторов электронных ключей пользователей при их воздействии на считыватели терминала.
- Постоянный контроль электропитания и GSM-сигнала с информированием клиента.
- Сохранение режимов работы устройства и состояния его выходов после отключения/восстановления питания.
- Запись событий во внутренний «черный ящик».
- Аудиоконтроль охраняемого объекта при возникновении тревожного состояния или по запросу клиента.
- Настройка интервала отправки «сигналов жизни» от 1 мин. и отслеживание их на Пульте Централизованного наблюдения (програмное обеспечение ПЧН приобретается отдельно).



3. Основные понятия и определения

Терминал – техническое устройство с программным обеспечением выполняющие ряд функции, описанных в данном руководстве, и осуществляющие связь с пользователями системы посредством GSM-модема.

Профиль – часть внутренней энергонезависимой памяти терминала, хранящая настройки параметров, определяющих режимы работы терминала.

Администрирование – возможность управления работой и конфигурацией терминала одним из пользователей системы (администратором).

Рассылка SMS-сообщений – отправление терминалом SMS-сообщений пользователям системы, для которых, в профиле терминала, разрешена обработка источников отправляемых сообщений.

Имя-псевдоним – альтернативное название входов или выходов терминала удобное для восприятия информации пользователями системы. Имена-псевдонимы используется в расширенном формате отправляемого SMS-сообщения или для управления посредством SMS команд.

Тревожное событие – событие, возникающее при обнаружение активного состояния на активированных входах терминала. Реакцией на тревожное событие будет рассылка тревожного SMS-сообщения, с указанием причины возникновения события и выполнение действий на выходах терминала, если они запрограммированы для активного состояния тревожного входа.

Системное событие – событие, не связанное с обнаружением тревожного состояния на охранных входах терминала, возникновение события не зависит от состояния охраны терминала. Реакцией на системное событие служит, как правило, только рассылка SMS-сообщения. Реакция на выходах не предусмотрена, исключением являются системные события: «Постановка терминала на охрану» и «Снятие терминала с охраны».

Охранная сессия – период времени, в течение которого терминал находится в режиме «Охрана». Началом охранной сессии считается переход терминала в состояние «Охрана», а завершением, переход в режим «Снят с охраны».

Самотестирование – процесс выявления неисправностей или тревожных состояний на входе при взятии его под охрану. В случае отказа по окончанию тестирования, происходит обход неисправного входа, т.е. блокируется его обработка до начала следующей охранной сессии.

Тревожная кнопка – логический вход терминала, обнаружение на котором, активного состояния, приводит к рассылке тревожного SMS-сообщения не зависимо от статуса охраны.

Аудиоконтроль – дает возможность звукового контроля охраняемого помещения пользователям системы, при установлении соединения с терминалом, в режиме голосового звонка.

Электронный ключ – Устройство хранящее в электронном виде цифровой код-идентификатор и передающее его при взаимодействии (прямом контактном или электромагнитным бесконтактным) со считывателем электронных ключей. Примерами ЭК могут служить iButton/TouchMemory («кнопки», «таблетки») или бесконтактные карты Proximity.

Считыватели Электронных Ключей – Устройства, производящие снятие кодов-идентификаторов электронных ключей и их дальнейшую передачу по проводным линиям связи к контроллерам электронных ключей для распознавания и формирования действия.

Контроллер Электронных ключей – электронные устройства, производящие сравнение передаваемых на них со считывателей кодов-идентификаторов



электронных ключей с хранящимися в их памяти. Контроллер определяет является ли ключ «своим», уровень его доступа и инициирует определенную последовательность действий связанную с приемом этого кода-идентификатора.

Мастер Ключ (MasterKey) – электронный ключ, код-идентификатор которого не влияет на состояния выходов терминала, но переводит контроллер электронных ключей в режим добавления/удаления в его память кодов-идентификаторов электронных ключей пользователей.



4. Режимы работы устройства

4.1. Режим «Снят с охраны»

Переход в режим «Снят с охраны» осуществляется одним из способов:

- изменением состояния на входе терминала «Снятие» согласно настройки режима снятия/постановки терминала на охрану;
- отправкой SMS-команды или команды с ПЦН «Снять терминал с охраны»;
- активированием кнопки №2 «Снятие терминала с охраны» радиобрелка, если для радиобрелка задан режим «Охранный» или «Охранно-тревожный»;
- срабатыванием пользовательского ключа ТМ при включении режима ТМ «только снятие» или «постановка/снятие» с охраны.

При переходе терминала в режим «Снят с охраны» выполняются следующие действия:

- сбрасываются все тревожные состояния на входах;
- гаснут индикаторы «Охрана» и «Тревога»;
- выполняются действия на выходах, согласно настройкам режимов в профиле терминала;
- рассыпается сообщение «Терминал снят с охраны». Если терминал до перехода в режим «Снят с охраны» находился в состоянии постановки на охрану, но не был в режиме «Охрана», то SMS-сообщение «Терминал снят с охраны» не будет отправлено.

В этом режиме будут обрабатываться только «Круглосуточные» входы, а изменение состояния на других входах будет игнорироваться. Все остальные события, возникающие в этом режиме, будут обрабатываться согласно логики их обработки заложенной в профиле терминала.

4.2. Режим «Охрана»

Режим «Охрана» имеет несколько состояний: постановка терминала на охрану и собственно охрана.

Постановка терминала на охрану может быть вызвана:

- изменением состояния на входе терминала «Постановка» согласно настройки режима снятия/постановки терминала на охрану;
- получением SMS-команды или команды с ПЦН: «Поставить терминал под охрану»;
- активированием кнопки №1 «Постановка терминала на охрану» радиобрелка, если для радиобрелка задан режим «Охранный» или «Охранно-тревожный»;
- срабатыванием пользовательского ключа ТМ при включении режима ТМ «только постановка» или «постановка/снятие» с охраны.

При переходе в состояние постановки терминала на охрану выполняются следующие действия:

- выполняются действия на выходах, согласно настройкам режимов в профиле терминала;
- активируется задержка равная «Времени постановки терминала на охрану»;
- запускается процедура самотестирования;
- индикатор «Охрана» начинает быстро мигать (1 Гц).

По завершению задержки «Времени постановки терминала на охрану» устройство переходит в режим «Охрана», при этом выполняются следующие действия:

- индикатор «Охрана» начинает медленно мигать (0,5 Гц);
- по окончанию процедуры самотестирования отправляется SMS-сообщение «Статус постановки на охрану», содержащие информацию о состоянии внутренних объектов после тестирования;



В режиме «Охрана» разрешена обработка всех активных входов, если они успешно прошли тест при постановке. Если при постановке вход по какой-либо причине не прошел тест (в т.ч. Если его состояние отлично от заданного в профиле как «изначальное состояние входа»), то при переходе в состояние охраны терминал блокирует его обработку до следующей охранной сессии, с указанием в статусном сообщении причины отказа.

4.3. Состояние «Тревога»

Состояние «Тревога» может возникнуть в любом из режимов работы терминала. Причиной возникновения может послужить тревожное состояние на входе, обработка которого разрешена в текущем режиме работы терминала. При этом будут выполнены следующие действия:

- индикатор «Тревога» начнет быстро мигать (1 Гц);
- выполнение действий на выходах, сконфигурированных в профиле для активного состояния на входе;
- рассылка тревожного SMS-сообщения, с указанием источника и причины возникновения тревоги.

Возникновение других тревожных событий будет приводить только к рассылки тревожных SMS-сообщений, если это предусмотрено логикой обработки события заданной в профиле терминала.

Любой из вышеозначенных режимов сохраняется в энергонезависимой памяти устройства и при отключении электропитания. После восстановления питания устройство возобновляет свою работу в том же режиме в котором оно находилось до отключения от электропитания.



5. Работа с SMS-сообщениями

5.1. Синтаксис отправляемых SMS-сообщений

Тревожные

Таблица 1

Имя аргумента	Значение	Описание	Примечание
Terminal	Reboot	Перезагрузка терминала	Системное событие
	Fail	Аналоговый шлейф не готов (разрыв шлейфа)	Не прошел тест
	KZ	Короткое замыкание на входе аналогового шлейфа	Не прошел тест
	Left	Произошел переход по левому фронту на аналоговом шлейфе (размыкание контакта)	—
	Right	Произошел переход по правому фронту на аналоговом шлейфе	— —
Сухие Контакты SN1...SN8 или их псевдонимы	Left	Произошел переход по левому фронту на цифровом входе (размыкание контакта)	—
	Right	Произошел переход по правому фронту на цифровом входе (замыкание контакта)	— —
GSM Signal	Low [time]	Время падения уровня сигнала ниже критической отметки	Системное событие
	High [time]	Время восстановления сигнала выше критической отметки	Системное событие
Ext. power	low	Падение уровня внешнего питания	Системное событие
	high	Восстановление внешнего питания	Системное событие
Charm	Alarm	Тревога с радиобрелка	Системное событие
Box	Open	Вскрыт корпус устройства	Системное событие

Информативные

Таблица 2

Имя источника	Событие	Описание	Примечание
Client	status	Статус клиента	(см. формат сообщений)
Device	status	Полный статус устройства	(см. формат сообщений)

Продолжение Таблицы 2



Имя источника	Событие	Описание	Примечание
LP1...LP4	Prof	Профиль аналогового шлейфа	(см. формат сообщений)
SN1...SN8	Prof	Профиль цифрового входа	(см. формат сообщений)
OUT1..OUT4	Prof	Профиль выхода	(см. формат сообщений)
CL1...CL8	Prof	Профиль клиента	(см. формат сообщений)
Terminal	Parametrs	Профиль параметров терминала	(см. формат сообщений)
Charm	Erase Complete	Стирание всех брелоков из памяти	
	Block	Работа радиобрелков заблокирована	
	Unblock	Работа радиобрелков возобновлена	
	Fine Learn	Успешное обучение радиобрелоков	
	Replace Phone	Удаленная смена телефонного номера клиента	
Health Signal		Истек интервал контрольной точки	
Guard	[Status] / On*	Постановка терминала на охрану	
	OFF	Терминал снят с охраны	
Key	Block All;	Модуль электронных ключей заблокирован	
	Unblock All;	Модуль электронных ключей разблокирован	
	master:[ID]	Новый идентификатор Мастер ключа:[№идентификатор]	
	Add:[ID]	Добавлен Ключ: [№идентификатор]	
	Del:[ID]	Удален ключ: [№идентификатор]	
	passed:[ID]	Сработал ключ: [№идентификатор]	

* Стандартный режим/Расширенный режим

5.2. Структура SMS сообщений

1) Структура тревожных сообщений:

Время	Имя источника	Для входов '='	Событие	Конец сообщения ','
		Для остальных ''		

Пример:
а) 19:05



*LP1=Right;
b)01:02
Terminal Reboot;*

2) Структура информативных сообщений

2.1) Статус:

Время	Заголовок ‘:’	Guard ON/OFF ‘;’	Имя входов ‘=’	ON/OFF/AL ‘;’	Имя выходов ‘=’	ON/OFF/IMP ‘;’
-------	---------------	------------------	----------------	---------------	-----------------	----------------

Пример:

12:00

Client Status:

GuardON;LP1=ON;LP2=OFF;LP3=OFF;LP4=OFF;SN1=ON; SN2=ON; SN3=ON; SN4=ON; SN5=ON; SN6=ON; SN7=AL; SN8=AL;OUT1=ON;OUT2=IMP;

2.2) Профиль:

Время	Заголовок ‘:’ (имя по умолчанию)	Псевдоним ‘,’	Параметр ‘=’	Значение ‘,’
-------	-------------------------------------	---------------	--------------	--------------

Пример:

15:25

LP1 Prof:

LP1,TmB=1,TmQ=0,TmA=0,Act=4,Pas=8,Max=76,Min=30,En=1,24=0,WE=2

5.3. SMS команды

SMS команды составляются пользователями системы символами латинского алфавита, без пробела или дополнительных символов между именем и действием в команде. В качестве имени в команде можно указать имя-псевдоним объекта, к которому адресуется команда.

В одном SMS-сообщении может содержаться несколько команд разделенных пробелами. Очередность выполнения команд будет начинаться с первой команды в SMS-сообщении.

SMS команды

Таблица 3

Имя	Действие	Описание	Прим.
*LP1...LP4 (либо псевдонимы)	ON	Активировать аналоговый шлейф с номером	
	OFF	Деактивировать аналоговый шлейф с номером	
	GET	Запросить профиль аналогового шлейфа с номером	
LPALL	Y	Активировать все аналоговые шлейфы	
	N	Деактивировать все аналоговые шлейфы	
*SN1...SN8 (либо псевдонимы)	GET	Запросить профиль цифрового входа с номером	



Продолжение Таблицы 3

Имя	Действие	Описание	Прим.
*OUT1... OUT4 (либо псевдонимы)	ON	Включить выход с номером	
	OFF	Выключить выход с номером	
	IMP	Задать импульсный режим выходу с номером	
	GET	Запросить профиль выхода с номером	
*CL1...CL8	GET	Запросить профиль клиента с номером	
GUARD	Y	Поставить терминал под охрану	
	N	Снять терминал с охраны	
STAT		Запросить статус клиента	
*DSTAT		Запросить статус устройства	
*CH	ERASE	Стирание из памяти всех радиобрелков	
	BLC	Заблокировать работу радиобрелков	
	UNBLC	Возобновить работу радиобрелков	
	LEARN	Запустить процедуру обучения брелков	
*KEY	BLC	Заблокировать модуль электронных ключей	
	UNBLC	Разблокировать модуль электронных ключей	
	ERASE:[ID]	Удалить ключ [№идентификатор ключа]	

*Доступны только администратору.



6. Настройка параметров работы устройства

6.1. Программирование SIM-карты

Программирование SIM-карты требуется для правильной и надежной работы терминала. SIM-карта в комплект поставки не входит, а приобретается у местного оператора.

Процедура программирование SIM-карты состоит из нескольких этапов:

Этап 1: SIM-карту необходимо вставить в любой сотовый телефон и включить его. Далее удалите все хранящиеся в памяти SIM-карты SMS-сообщения и все номера из «Телефонной книги». Все действия необходимо производить в соответствии с инструкцией сотового телефона.

Этап 2: Отключите запрос PIN-кода, пользуясь инструкцией сотового телефона. **Убедитесь, что запрос PIN-кода отключен.** Для этого выключите и включите заново сотовый телефон, если при включении телефона нет запроса PIN-кода, то действия выполнены правильно.

Этап 3: Этот этап необходимо выполнять только в том случае, если с помощью сервисной программы не были заданы телефонные номера «Клиентов». Это необходимо для работы терминала посредством GSM-модема: прием и передача SMS-сообщений, аудиоконтроль. Номера «Клиентов» вводятся поочередно начиная с первой ячейки памяти «Телефонной книги» SIM-карты в общепринятом международном или междугородном формате, например «+79102223344» (если номер не соответствует данным форматам – он игнорируется!). Телефонный номер сохраненный в первой ячейки памяти дает «Клиенту» с этим номером права «Администратора». Максимально терминал обрабатывает первые восемь ячеек памяти, т.е. восемь телефонных номеров.

Этап 4: Выключите сотовый телефон и извлеките SIM-карту.

УБЕДИТЕСЬ, ЧТО ПИТАНИЕ ТЕРМИНАЛА ОТКЛЮЧЕНО!

Извлеките держатель SIM-карты из терминала, нажав заостренным предметом на желтый фиксатор держателя. Вставьте SIM-карту в держатель, соблюдая правильность позиционирования карты в держателе. Установите держатель с SIM-картой обратно в гнездо терминала.



6.2. Работа с радиобрелками

6.2.1. Изменение режима работы радиомодуля.

Радиомодуль может находиться в одном из состояний (режим работы):

- нормальный режим;
- режим блокирования работы радиомодуля;
- режим блокирования работы радиобрелков;
- режим обучения радиобрелков.

Изначально в памяти терминала нет ни одного серийного номера радиобрелка и радиомодуль находится в режиме блокирования работы. В нормальный режим работы радиомодуль можно перевести, запустив процедуру обучения радиобрелков и сохранить хотя бы один серийный номер радиобрелка.

Блокирование работы радиомодуля можно осуществить – отправив SMS-сообщение с командой «Стереть радиобрелки», после чего из памяти терминала будут удалены все ранее сохраненные серийные номера радиобрелков и радиомодуль перейдет в начальное состояние.

Блокирование работы радиобрелков осуществляется тоже отправкой SMS-сообщения с командой «Заблокировать радиобрелки», далее возобновить нормальный режим работы можно только с помощью SMS-сообщения с командой «Разблокировать радиобрелки».

6.2.2. Процедура обучения радиобрелков.

Процедура обучения подразумевает под собой строгую последовательность действий, после успешного завершения которых, в память терминала сохраняются серийные номера обученных радиобрелков.

Последовательность действий для обучения радиобрелков:

1. Перевести терминал в режим «Снят с охраны».
2. Выключить терминал – отключить резервное и основное питание.
3. Замкнуть вывод «Цифровой вход №6» с выводом «Общий».
4. Включить терминал – подать питание.
5. Выдержав паузу в 8 секунд -> разомкнуть вывод «Цифровой вход №6».

Индикатор «Охрана» начинает быстро мигать с частотой 10 Гц.

Начинается отсчет интервала времени «Продолжительность обучения» равному 20 секундам.

6. Активировать радиобрелок – нажав любую кнопку.

Индикатор «Охрана» мигнет такое количество раз, которое соответствует текущему номеру сохраненного радиобрелка.

7. Если необходимо - активируйте следующий радиобрелок.

Возможна запись только 4-х разных радиобрелков.

8. По истечению интервала времени «Продолжительность обучения» терминал перейдет в режим «Снят с охраны». Произойдет сохранение серийных номеров обученных радиобрелков в память терминала.



Если за время «Продолжительность обучения» не было активировано ни одного радиобрелка, то произойдет стирание ранее сохраненных серийных номеров радиобрелков из памяти терминала и будет выполнен режим блокирования работы радиомодуля.

9. Отправлено сообщение с информацией о состоянии режима работы радиомодуля. В случае успешного обучения в сообщении будет указано количество успешно обученных радиобрелков.



6.3. Работа с электронными ключами и картами доступа.

Терминал ТСИ-03 имеет возможность осуществлять функции Системы Контроля и Управления Доступом. Разграничение доступа осуществляется посредством радиобрелоков со статическим кодом, электронных ключей TouchMemory и магнитных карт Proximity стандарта Wiegand (при использовании специализированных контроллеров IronLogic имеющих выходной протокол Dallas1990).

Внутренняя память терминала хранит до 128 ключей пользователей, с помощью которых можно управлять исполнительными устройствами (электрозамками, системами оповещения и др.), осуществлять постановку/снятие терминала с охраны и отправку сообщений с идентификатором пользователя на центральный пульт диспетчерского центра.

Также имеется группа из 128 идентификаторов ключей ЧОП/ГБР. Данные идентификаторы не оказывают влияния на работу терминала, его режимы или производимые им действия, однако они распознаются терминалом и пересыпаются им на ПЦН также как и ключи пользователей.

Каждая группа ключей имеет независимую базу, управляемую двумя различными мастер-ключами, один из которых хранится в ЧОП, другой у владельца объекта.

6.3.1. Изменение режима работы модуля электронных ключей.

Модуль MicroLan может находиться в одном из состояний (режимов работы):

- рабочий (нормальный) режим;
- режим обучения MasterKey;
- режим изменения состава группы ключей доступа;
- режим блокировки модуля TouchMemory.

Изначально в памяти терминала нет ни одного идентификатора ключа пользователя и MasterKey и модуль находится в режиме блокирования работы. В нормальный режим работы радиомодуль можно перевести, запустив процедуру изменения MasterKey и сохранить его идентификатор.

ВАЖНО: При завершении процедуры смены ключа MasterKey вся информация обо всех остальных ключах пользователей будет удалена из памяти терминала! Даже если будет введен тот же MasterKey.

Режим изменения состава группы инициируется после прикосновения ключом MasterKey к контактору TouchMemory или считывателю Proximity/Wiegand. Данный режим характеризуется поочередным миганием красного и синего индикаторов на корпусе терминала. Если в течение 20 секунд после запуска этого режима к контактору/считывателю не будет поднесено ни одного ключа терминал вернется в нормальный рабочий режим. Если терминал находится в данном режиме, то идентификатор любого ключа, воздействующего на считыватель будет либо записан в память устройства (если такой идентификатор отсутствует) либо удален из него (если такой идентификатор уже есть).

Блокирование работы модуля электронных ключей осуществляется отправкой SMS-сообщения с командой «Заблокировать модуль ключей», далее возобновить нормальный режим работы можно только с помощью SMS-сообщения с командой «Разблокировать модуль ключей».



В случае заблокированного модуля электронных ключей считывание ключей пользователей и ключей ЧОП/ГБР не производится, передачи идентификаторов ключа на ПЧН также производится не будет.

6.3.2. Процедура изменения MasterKey.

Процедура изменения подразумевает под собой строгую последовательность действий, после успешного завершения которых, в память терминала сохраняется серийный номер **MasterKey**.

Последовательность действий для изменения MasterKey:

1. Перевести терминал в режим «Снят с охраны».
2. Выключить терминал – отключить резервное и основное питание.
3. а) Для изменения Мастер-Ключа пользовательской группы - замкнуть pin/контакт «+» «Цифрового входа №5» с выводом «Общий».
б) Для изменения Мастер-Ключа группы ключей ЧОП/ГБР- замкнуть pin/контакт «+» «Цифрового входа №4» с выводом «Общий».
4. Включить терминал – подать питание.
5. Выдержав паузу в 8 секунд разомкнуть pin/контакт «+» «Цифрового входа» и «Общий» pin/контакт.
6. Индикатор «Статус» (синий) начинает быстро мигать с частотой 10 Гц. Если этого не произошло повторить шаги 2..5.
7. Начинается отсчет интервала времени «Продолжительность обучения» равному 20 секундам.
8. Занести Идентификатор **MasterKey** – приложить его к считывателю.
9. Индикатор «Статус» (синий) включится на 2 секунды. Произойдет сохранение идентификатора **MasterKey** в память терминала.
10. По истечению интервала времени «Продолжительность обучения» терминал перейдет в режим «Снят с охраны».
11. Отправлено сообщение с информацией о состоянии режима работы модуля электронных ключей. В случае успешного обучения в сообщении будет указан код-идентификатор нового Мастер ключа.

6.3.3.Процедура изменения базы кодов-идентификаторов электронных ключей.

Процедура изменения подразумевает под собой строгую последовательность действий, после успешного завершения которых, в память терминала сохраняется или из памяти удаляется код-идентификатор электронного ключа пользователя/ключа ЧОП/ГБР.

Последовательность действий для обучения радиобрелков:

1. Перевести терминал в режим «Снят с охраны».
2. Приложить к считывателю электронных ключей **MasterKey**
3. Индикатор «Статус» (синий) и «Тревога» (красный) начинают быстро переменно мигать с частотой 10 Гц.
4. Начинается отсчет интервала времени «Продолжительность обучения» равному 20 секундам.



5. Приложить электронный ключ пользователя к считывателю электронных ключей.
 - 5.1 В случае если данный код-идентификатор уже содержится в памяти контроллера, то он будет удален из нее. В подтверждение этого синий индикатор погаснет, а красный загорится на 2 секунды.
 - 5.2 В случае если данный код-идентификатор отсутствует в памяти контроллера, то он будет в нее добавлен. В подтверждение этого красный индикатор погаснет, а синий загорится на 2 секунды.
 - 5.3 Интервал «продолжительность обучения» начнется заново.
6. Повторить процедуру п.5 для всех электронных ключей, внимательно отслеживая реакцию индикаторов.
7. По истечению интервала времени «Продолжительность обучения» терминал перейдет в режим «Снят с охраны».
8. Отправлено сообщение с информацией о состоянии режима работы модуля электронных ключей. В случае успешного обучения в сообщении будет указан код-идентификатор нового ключа пользователя.



6.4. Сервисная программа для настройки параметров терминала

Сервисная программа для настройки параметров терминала предназначена для конфигурирования профильной информации и сохранения ее во внутреннюю память терминала.

Для начала программирования профиля нужно подключить ПК к терминалу при помощи USB-кабеля. Питание к терминалу можно не подключать, если производится только сохранение профильной информации в терминал.

После подключения терминала к компьютеру, в диспетчере устройств в разделе USB устройств и/или СОМ-портов появятся «неизвестные устройства» обозначенные желтыми предупредительными знаками. Для дальнейшей работы с терминалом потребуется установить драйвер контроллера. Он находится в папке /drv на компакт-диске с программным обеспечением. Запустив его необходимо нажать клавишу «Next» в первом окне, поставить флажок согласия с требованиями лицензионного соглашения в следующем окне, после чего опять же нажать «Next», выбрать путь для распаковки файлов (желательно оставить предложенный программой) и опять нажать «Next». После успешной распаковки файлов вы увидите следующее окно:

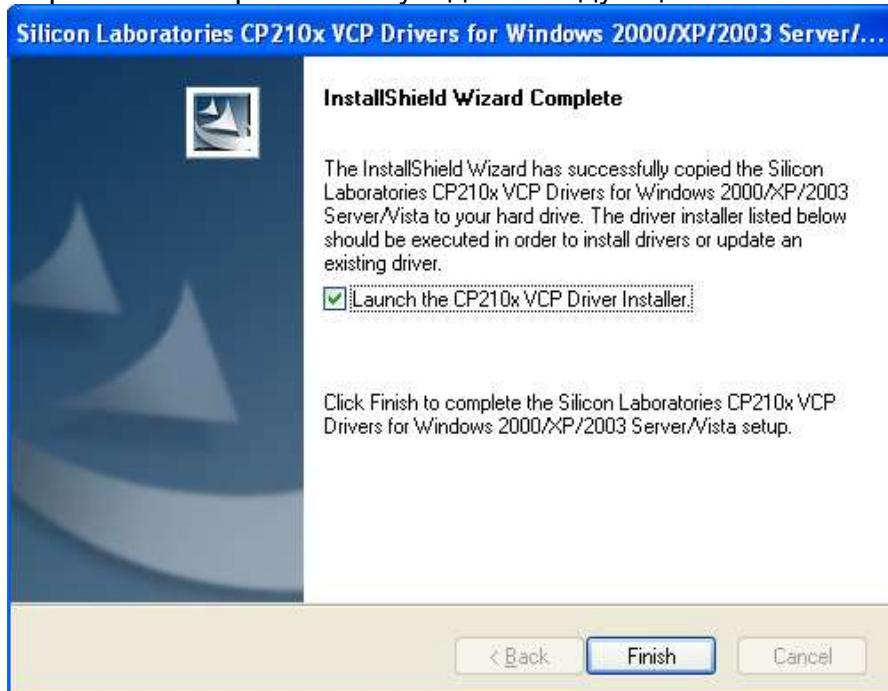


Рисунок 1. Окно окончания распаковки драйверов.

Данное окно обозначает лишь успешную распаковку драйверов, но не их установку в систему. Для того, чтобы произвести установку, необходимо установить флажок около надписи Launch The CP210x VCP Driver Installer и только после этого нажать клавишу Finish.

После этого начнется собственно установка Драйверов, о чем подтвердит Вам окно:

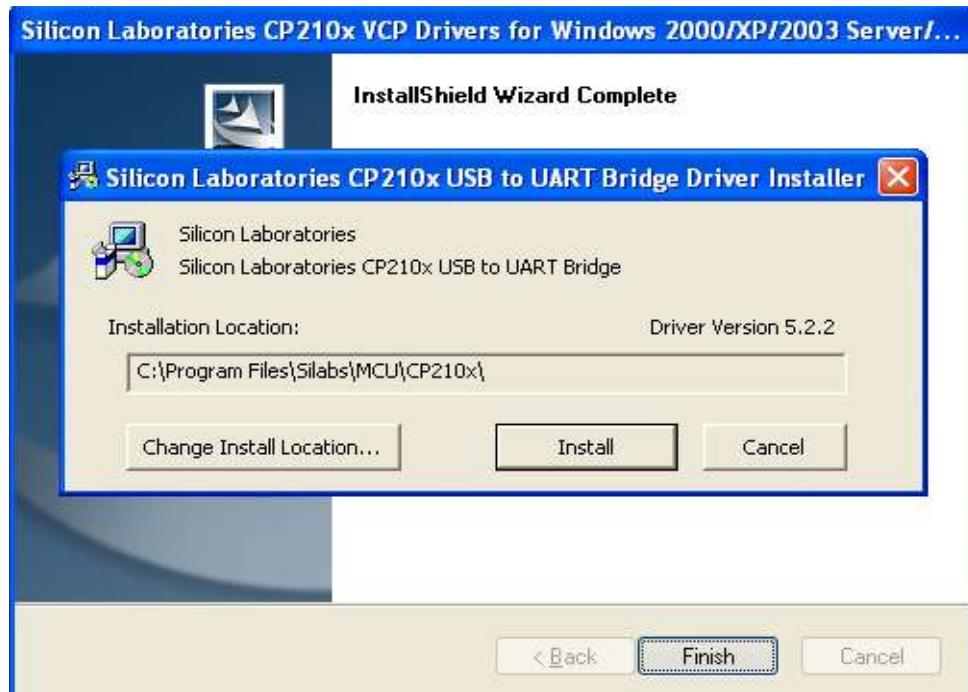


Рисунок 2. Окно выбора места установки драйверов.

В данном окне можно изменить путь установки драйвера (не рекомендуется) после чего нажав клавишу **Install** запустить инсталляцию.

После завершения инсталляции драйверов они все еще не до конца могут прописаться в Вашей системе. Для того, чтобы убедиться в успехе, необходимо посмотреть «Свойства Компьютера — Оборудование — Диспетчер устройств». Если около устройства с названием **CP2102 USB-to-UART Bridge Controller** стоит желтый круг с черным восклицательным знаком, то вам нужно будет принудить Ваш ПК завершить установку.

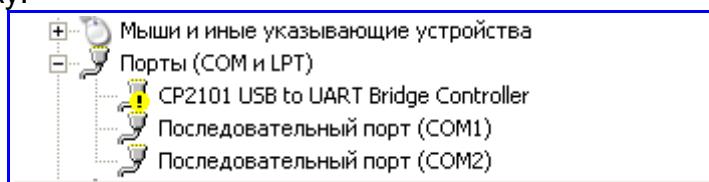


Рисунок 3. Диспетчер устройств. Предупреждение о неполной установке драйвера.

Для этого необходимо Нажав правую клавишу мыши на устройстве выбрать пункт «Обновить драйвер ...», отказаться от подключения к узлу WindowsUpdate (пункт «Нет не в этот раз»), отказаться от автоматической установки (пункт «Установка из указанного места») и выбрать пункт «Не выполнять поиск. Я сам выберу нужный драйвер». Выбрав этот пункт и нажав далее вы должны увидеть список из единственного драйвера, соответствующем Вашему устройству, на котором нужно установить курсор и нажать «Далее».



После этого установка должна быть завершена, о чём будет свидетельствовать исчезновение знака предупреждения со строки устройства:

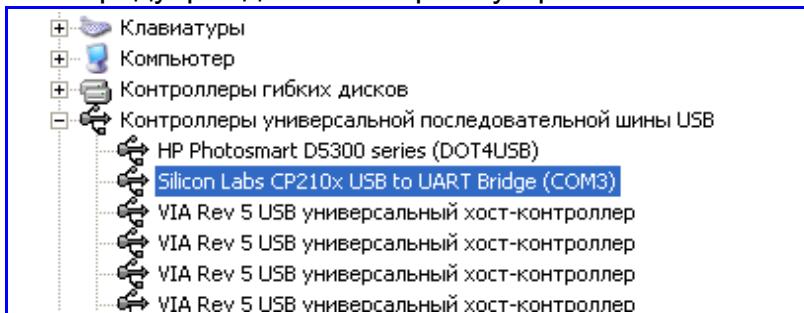


Рисунок 4. Диспетчер устройств. Успешная установка драйвера устройства.

В данной строке Вам также необходимо запомнить номер СОМ-порта, назначенного для обмена данными ПК с терминалом. На изображении это СОМ порт № 3.

Для установки собственно программы конфигурации Вам нужно запустить файл setup.exe из папки /util диска с ПО или выбрав пункт «установить сервисную утилиту» из меню автозапуска диска. Программа конфигурации будет расположена в «Пуск» - «Программы» - «Elebrain» — «SlyCenter 4» – «Сервисная утилита».

Первое, что нужно сделать запустив программу конфигурации - это правильно задать параметры соединения, это можно сделать, выбрав пункт меню «Операции -> Параметры соединения». Как правило, для установления соединения нужно только правильно задать номер СОМ-порта ПК, определенного при установке драйвера устройства и скорость обмена данными по этому СОМ-порту. При отклонении установленного значения скорости обмена от необходимого передача данных может происходить с ошибками или вовсе не осуществляться.

Рекомендуется устанавливать значение скорости порта равное 115200, отличное от значения по умолчанию (обычно равно 9600).

После установки новых параметров для их сохранения нажимаем клавишу «Применить».

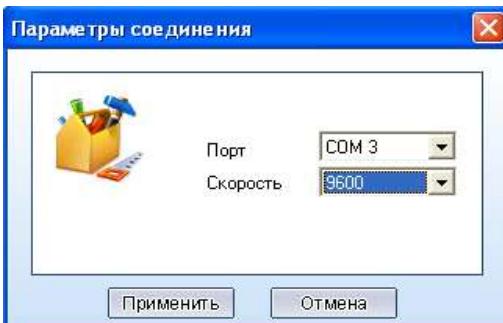


Рисунок 5. Настройка параметров соединения с терминалом.

6.4.1. Меню сервисной программы.

С помощью вкладки меню «Файл» можно загрузить раннее созданный профиль из файла с расширением .pfl или сохранить вновь созданную профильную конфигурацию в файл на ПК.

На вкладке меню «Операции» представлены команды, работающие по внутреннему протоколу с терминалом.

Выбрав «Операции -> Опросить информацию об устройстве» можно в шапке программы получить информацию о подключенном типе устройства, версии аппаратной части, версии программного обеспечения, а также получить ID терминала. Последний параметр может быть необходим для регистрации устройства в базе



данных сервера ПЧН SlyCenter 4. **Данный параметр может быть считан ТОЛЬКО при подключенном питании 12 В.**

Команда «Операции -> Перезапустить терминал» перезагружает подключенный терминал, тем самым, запуская внутреннюю программу с обновленным профилем.

После настройки параметров необходимым для пользователя (пользователей) образом или загрузив из файла необходимую конфигурацию её можно записать в терминал с помощью команды «Операции -> Записать данные в терминал». Важно отметить, что версия загружаемого профиля должна соответствовать (поддерживаться) версии аппаратной части и программного обеспечения терминала. Для вступления изменений в силу необходимо перезагрузить терминал.

Считать текущую конфигурацию терминала можно командой «Операции -> Прочитать данные из терминала». Все параметры будут доступны в сервисной программе.

При работе с терминалом посредством сервисной программы пользователю доступны для изменений следующие объекты логической структуры терминала:

- «Клиенты»
- «Общие настройки»
- «Параметры терминала»
- «Цифровые входы»
- «Аналоговые входы»
- «Выходы»
- «Параметры Связи»
- «Управление Доступом»

Каждый из этих объектов имеет ряд параметров, которые сохраняются в профиле терминала. От значений параметров сохраненных в профиле зависит алгоритм работы и выполняемые функции терминала.

6.4.2. Объект настройки «Клиенты»

Объект «Клиенты» описывает структуру хранящую настройки взаимодействия терминала с пользователями данной системы. В качестве «Клиентов» (пользователей) могут выступать: хозяин охраняемого объекта, персонал работающий на охраняемом объекте, удаленный диспетчерский центр. В терминале могут быть сохранены до восьми «Клиентов», причем можно выбрать одного «Клиента» с правами «Администратора».

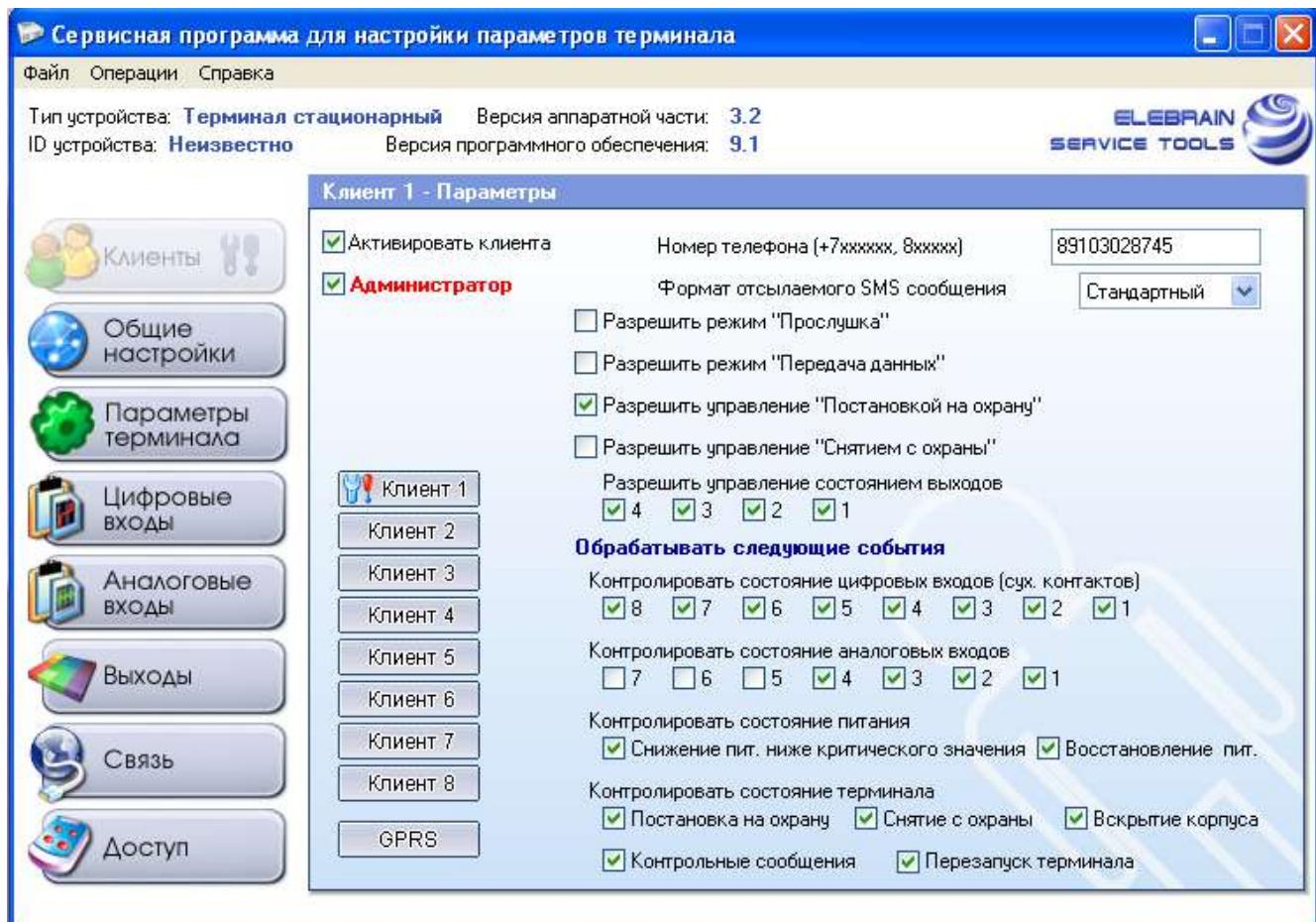


Рисунок 6. Окно настройки параметров клиентов терминала.

Гибкая настройка параметров «Клиентов» позволяет управлять или обрабатывать только те события, которые необходимы конкретному «Клиенту». Доступ в систему разрешен только тем пользователям, чьи телефонные номера сохранены в телефонном списке.

Активировать клиента можно только после ввода номера телефона абонента в соответствующем формате. **Если активен хотя бы один «Клиент», то телефонные номера, сохраненные в телефонной книге SIM-карты игнорируются!** Иначе управление и обработка событий будет осуществляться по телефонным номерам абонентов сохраненных в телефонной книге SIM-карты. (По умолчанию неактивен). Номера сохраненные на SIM-карте не отображаются в Сервисной программе.

Номер телефона задается в соответствии с общепринятым международным или междугородным форматом, например «+79102223344». (По умолчанию нет).

Администратор – это «Клиент» с расширенными правами на управление объектами. «Администратор» в отличие от остальных «Клиентов» имеет следующие права:

- удаленно активировать и дезактивировать любого «Клиента»;
- включить или отключить обработку всех «Цифровых входов»;
- включить или отключить обработку всех или конкретного «Аналогового входа»;
- заблокировать или восстановить обработку всех «Радиобрелков»;
- запустить процедуру обучения «Радиобрелков»;
- стереть из памяти терминала ранее сохраненные «Радиобрелки»;
- заблокировать или восстановить обработку всех электронных ключей;
- стереть из памяти терминала ранее сохраненные электронные ключи;
- подключить или разорвать подключение терминала через GPRS;
- запросить значения параметров объектов терминала.



«Администратор» может быть только один. (По умолчанию нет).

Формат отсылаемого SMS-сообщения может быть «Стандартным», тогда все исходящие SMS-сообщения содержат имена объектов присвоенных по умолчанию, например «LP1=ON; SN2=OFF; OUT1=IMP;». Если формат выбран как «Расширенный», тогда все исходящие SMS-сообщения содержат имена-псевдонимы объектов, например «DOOR=ON; WINDOW=OFF; RELE1=ON;». (По умолчанию «Стандартный»). Для клиента оснащенного Программой Диспетчерского Центра обязательно выбирать «Стандартный» Режим.

Если разрешен режим «Прослушка», то абонент в голосовом режиме с телефонного номера, которому разрешен режим, может установить соединения с терминалом для аудиоконтроля объекта. Интервал времени соединения задается в «Общих настройках». (По умолчанию запрещен).

ВНИМАНИЕ! При активной GPRS-сессии перехода в режим прослушка при звонке не происходит. Рекомендуется применять данную возможность при использовании только SMS-оповещений или при кратковременных GPRS-сессиях при сравнительно длительном периоде «сигналов жизни».

Разрешить управление «Постановкой на охрану» - команда о постановке на охрану от данного клиента терминалом обрабатываться не будет.

Разрешить управление «Снятием с охраны» - команда о снятии с охраны от данного клиента терминалом обрабатываться не будет

Разрешить управление состоянием выходов. Если параметр установлен для конкретного «Выхода», то «Клиент» получает возможность удаленно управлять состоянием этого «Выхода» по средствам SMS-сообщения, а так же получать информацию о состоянии «Выхода». (По умолчанию разрешено управление «Выходами» с №1 и №2).

Обрабатывать следующие события. Для конкретного «Клиента» необходимо разрешить обработку тех событий, информацию о которых ему нужно получать. (По умолчанию разрешено обрабатывать следующие состояния: «Цифровых входов» с № № 1 – 8, «Аналоговых входов» с №№ 1 – 4, внешнего питания, постановки и снятия с охраны, контрольные сообщения, перезапуск терминала).

В закладке **GPRS** содержатся все те же параметры, что и у обычных клиентов, однако они служат для определения полномочий администраторов ПЧН, подключающихся к терминалу по каналу GPRS от имени сервера Hive2server (Программный комплекс SlyCenter 4). Как результат, все эти параметры, за исключением двух, недоступны для изменения. Единственные два параметра, значение которых можно изменить в закладке **GPRS** — это **Разрешение на Постановку на охрану** и **Разрешение на снятие с охраны**.

6.4.3. Общие настройки

Объект «Общие настройки» описывает параметры одинаково определенные для всех «Клиентов».

В данном окне имеются две закладки: Закладка «Параметры» и отдельная закладка для «Видео».

Закладка «Параметры»

Пароль для удаленной замены телефонных номеров клиентов служит для смены одного телефонного номера «Клиента» на другой по средствам SMS-



сообщения в специальном формате. Например, для удаленной замены телефонных номеров «Клиентов» необходимо отправить терминалу SMS-сообщение в формате:

#пароль#текущий номер клиента#новый номер клиента

Например: «#password#+79102221111#89103334444»

В подтверждение попытки замены телефонных номеров «Клиентов» будет разослано SMS-сообщение содержащие информацию – «Кого меняют, кем меняют» на:

- номер с которого была попытка замены телефонных номеров;
- номер который был текущий (сменяемый);
- новый номер (сменяющий).

(По умолчанию пароль не задан нет).

Внимание! Пароль не может быть короче 4-х символов. Пароль является регистрозависимым, т.е. PassWord не равен password и не равен PASSWORD.

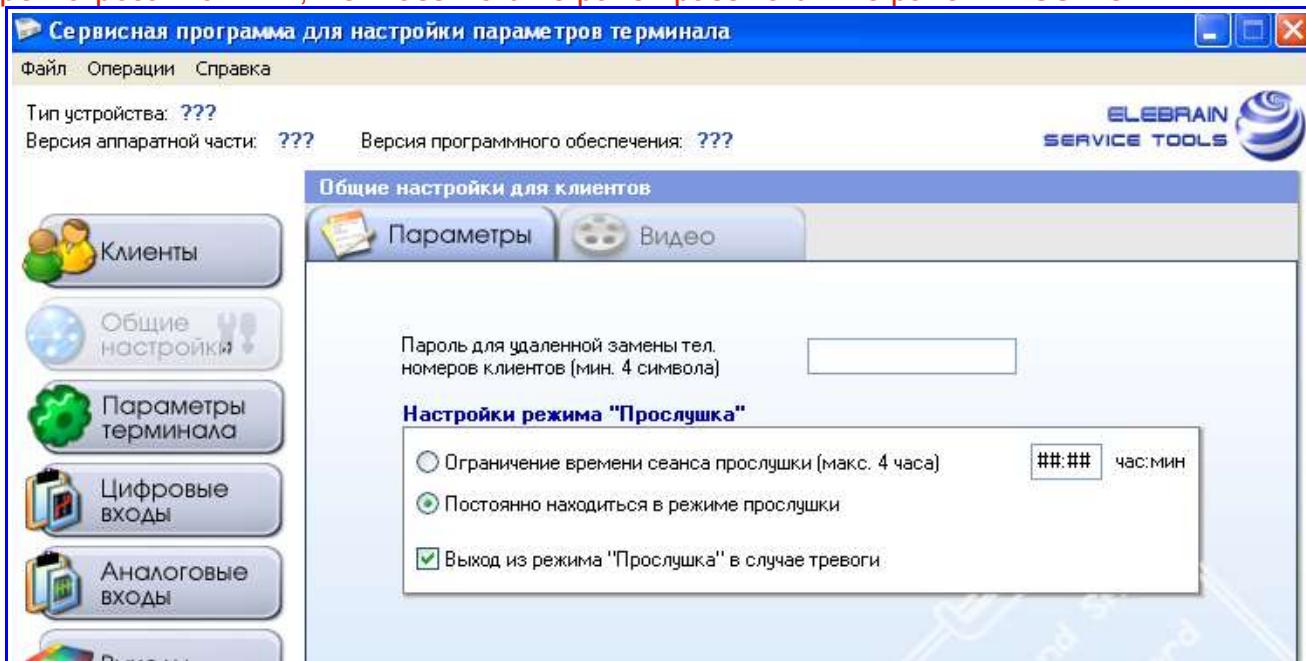


Рисунок 7. Окно общих настроек терминала. Параметры.

Если **ограничение времени сеанса прослушки** имеет значение в интервале от 0 до 4 часов, то по истечении этого интервала времени терминал обрывает соединение с клиентом. (По умолчанию нет).

Если активен параметр **выход из режима «Прослушка» в случае тревоги**, то при возникновении тревожной ситуации терминал также обрывает соединение с клиентом для отправки тревожного SMS-сообщения. (По умолчанию активен).

6.4.4. Закладка «Видео»

В данной закладке можно предварительно протестировать и оценить возможности подключаемой к терминалу через разъем RS-232 цифровой видеокамеры, а также настроить параметры автоматической отправки изображений.

Окно и параметры текущего изображения, статус-бар его получения и кнопка «Получить» служат для проверки работоспособности подключаемой камеры и настройка ее фокуса/резкости.

После нажатия кнопки «Получить» начнется процесс передачи изображения от камеры на персональный компьютер. Данный процесс будет сопровождаться

НТЦ «Элебрейн», г.Орел, 2008

www.elebrain.ru, e-mail: info@elebrain.ru



изменением строки «Состояние» и значением параметров «Пакет». Значение параметра «Пакетов» будет равно общему количеству информационных пакетов необходимых для создания полноценного изображения. Данные параметры неизменны и устанавливаются производителем. Предустановленный размер изображения 160x128. При запросе с удаленного сервера терминал поддерживает также изображения 640x480 , 320x240 и 80x64.

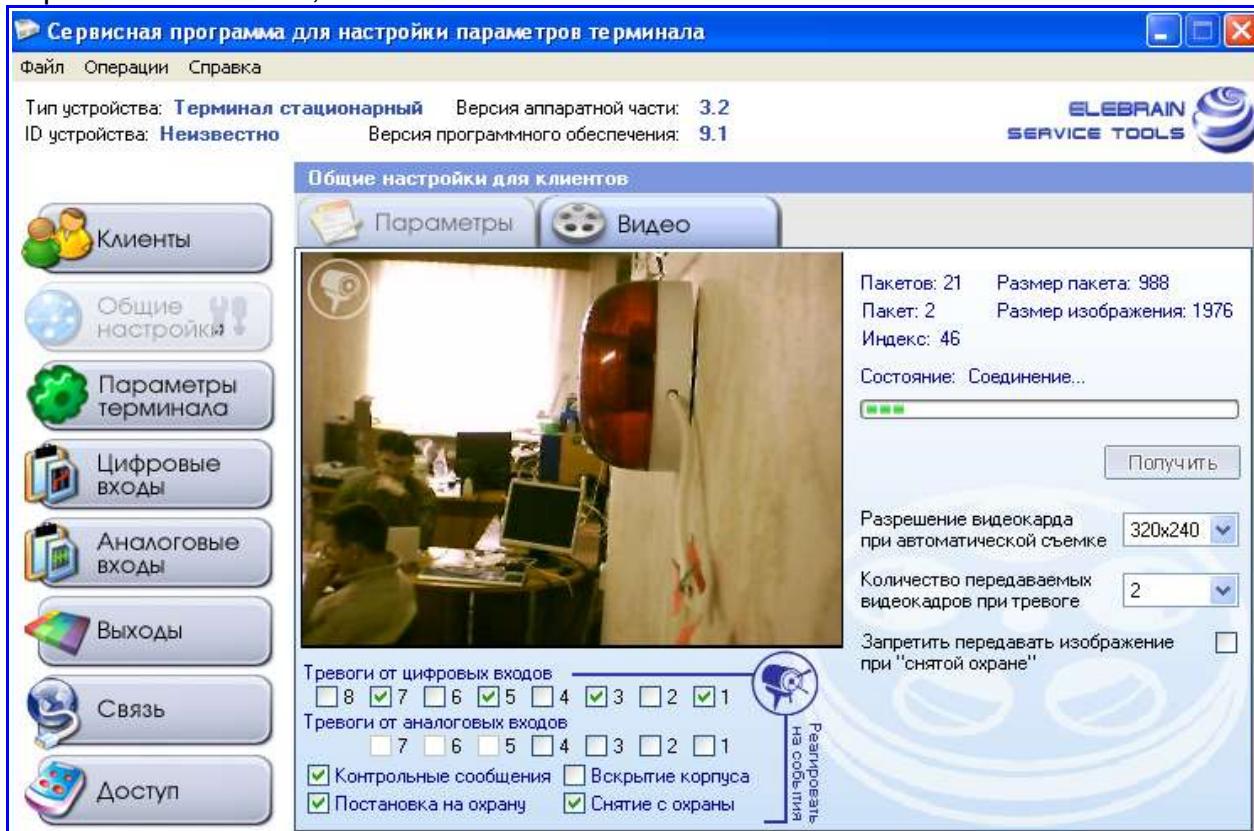


Рисунок 8. Окно общих настроек терминала. Видео.

Группа параметров Реагировать на события — устанавливает взаимосвязь (маршрутизацию) между тревожными и системными событиями регистрируемыми терминалом и фактом формирования и отправки изображений с камеры подключенной к терминалу.

Тревоги от цифровых входов / Тревоги на аналоговых входах — возникновение тревоги на любом из цифровых / аналоговых входов отмеченный флагком будет инициировать процедуру автоматической съемки

Контрольные сообщения — вместе с каждым «сигналом жизни» будет формироваться изображение (серия изображений) отправляемых на сервер

Вскрытие корпуса — при вскрытии корпуса будет сформировано и отправлено изображение. Имеет смысл при камере направленной на прибор или напосредственно рядом с ним.

Постановка на охрану — после постановки на охрану терминал сделает серию снимков и отправит их на сервер

Снятие с охраны — при снятии с охраны терминал произведет серию снимков и отправит их на сервер.

Разрешение видеокадра при автоматической съемке — устанавливает разрешение (а значит и размер) кадра, который будет передан на сервер терминалом при возникновении определенного события

Количество передаваемых видеокадров при событии (1/2/3) — Количество кадров которые будут переданы на сервер терминалом при возникновении определенного события



Запретить получать видеокадр при снятой охране — данный флажок служит для того, чтобы исключить излишнее вмешательство со стороны как пользователей так и сотрудников охранно-мониторинговых служб в личную и деловую жизнь владельцев, обитателей и сотрудников охраняемых объектов. При активации данного параметра терминал отвергнет любой запрос на получение видеоизображения сервером, если при этом он не будет находиться в режиме «на охране».

Исключение составляют кадры формируемые терминалом самостоятельно по «снятию с охраны», «постановке на охрану», «вскрытию корпуса» или «контрольные сообщения» («сигналы жизни»). В случае, если какое-то из этих событий отмечено флагом, то изображение по отмеченному событию будет отсылаться несмотря на установленный запрет.

6.4.5. Объект настройки «Параметры терминала»

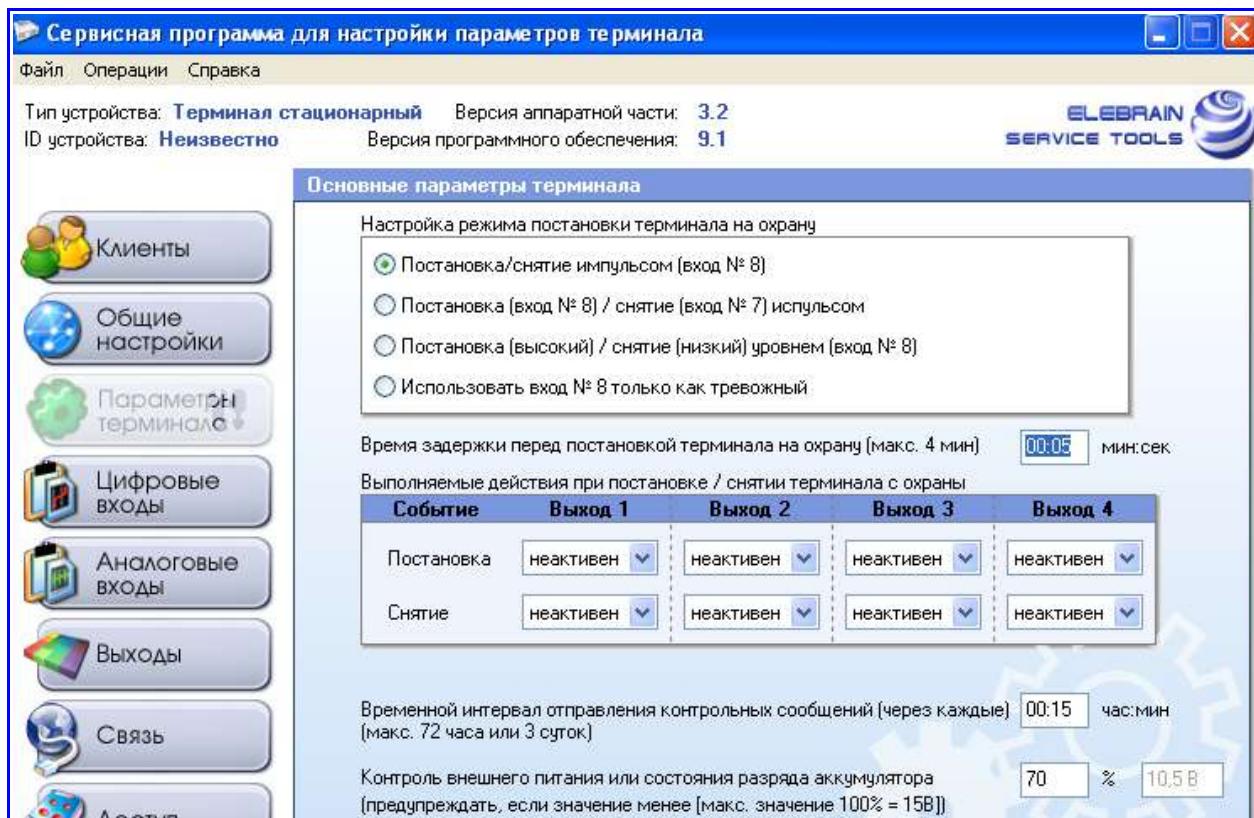


Рисунок 9. Окно параметров терминала.

В зависимости от **настройки режима снятия/постановки терминала на охрану** можно сконфигурировать для пользователей системы удобный и надежный (устойчивый к злонамеренному обходу охранных алгоритмов) способ внешней постановки на охрану и снятия терминала с охраны.

- если выбран режим «Постановка/снятие импульсом (вход №8)», то при каждом переходе из высокого уровня в низкий на «Цифровом входе» №8 будет происходить смена режима (состояния) охраны терминала.

- если выбран режим «Постановка (вход № 8)/снятие (вход №7) импульсом», то при переходе из высокого уровня в низкий на «Цифровом входе» №8 будет происходить постановка терминала на охрану (если предыдущее состояние терминала «Снят с охраны»). А при переходе из высокого уровня в низкий на «Цифровом входе» №7 будет происходить снятие терминала с охраны (если предыдущее состояние терминала «Поставлен на охрану»).



- если выбран режим «Постановка (высокий)/снятие (низкий) уровнем (вход №8)», то при переходе из высокого уровня в низкий на «Цифровом входе» №8 будет происходить снятие терминала с охраны, а при переходе из низкого уровня в высокий на «Цифровом входе» №8 будет происходить постановка терминала на охрану.

- если выбран режим «Использовать вход №8 только как тревожный», то цифровой вход №8 будет использоваться для подключения датчиков, а начало/завершение охранной сессии будет инициализироваться радиобрелками, командами оператора или электронными ключами.

(По умолчанию «Постановка/снятие импульсом (вход №8)»).

Время постановки терминала на охрану, как правило, задается для возможности покинуть охраняемый объект, не вызывая тревог от охраняемых зон. Так же этот интервал времени может использоваться для самонастройки датчиков и выхода их в дежурный режим. Например, установив в «Действиях при постановке» включить «Выход» №1 и задав «Время постановки терминала на охрану» равным 1 минуты, можно завести питание активных датчиков через выход №1, таким образом, дать активным датчикам самонастроится и начать опрашивать их, когда они выйдут в дежурный режим работы. (По умолчанию 5 сек.).

Для каждого «Выхода» можно задать следующие **выполняемые действия при постановке или снятии терминала с охраны**: включить, выключить или задать импульсный режим в соответствии с «Настройками работы импульсного режима» для конкретного «Выхода». (По умолчанию неактивен).

По истечению **временного интервала отправления контрольных сообщений** терминал формирует и рассыпает контрольные SMS либо GPRS сообщения («Сигналы жизни»). Минимальное значение интервала – 1 минута (По умолчанию 24 часа).

При расчете временных интервалов рассчитывайте не только важность объекта охраны, но и затраты на отсылку данных «Сигналов Жизни» всем заинтересованным клиентам по доступным каналам связи.

ВАЖНО! В случае использования GPRS-канала как основного рекомендуется использовать данный параметр как дополнительное средство повышения надежности канала связи. GPRS-сессии могут в различных регионах и периоды времени отличаться нестабильностью, как результат — сессия с высокой длительностью может «зависеть» по вине оператора сотовой связи или быть недоступна для терминала. Наиболее эффективное средство борьбы с этим явлением — переустановление сессии. Для этого необходимо комбинировать параметр период «сигналов жизни» и параметр «Длительность сессии» в закладке «Связь». Установив период сигналов жизни чуть больше длительности сессии можно добиться того, что после истечения длительности сессии терминал будет рвать соединение с базовой станцией сотовой связи, но уже через короткий промежуток времени, равный разнице периодов длительности сессии и периода «сигналов жизни», он будет устанавливать новую сессию.

Если задано значение величины разряда аккумулятора больше нуля, то при величине разряда аккумулятора меньшей заданного значения, терминал будет формировать тревожное сообщение о разряде подключенного аккумулятора либо о падении питающего напряжения ниже определенного значения.

6.4.6. Объект настройки «Цифровые входы»

Если **вход активирован**, то разрешается обработка терминалом состояния на входе. Если данный параметр неактивен, то обработка состояния входа производится не будет. (По умолчанию активен).



Если вход **выбран круглосуточным и вход активен**, то обработка состояния на этом входе происходит независимо от состояния охраны терминала. (По умолчанию некруглосуточный).

Название входа – имя-псевдоним входа длиной до 8 символов, используется в расширенном формате SMS-сообщения. В стандартном формате SMS-сообщения имя «Цифрового входа» соответствует «SN+номер входа». (По умолчанию «SN+номер входа»).

Режим работы входа указывает на то, какие состояния на входе необходимо обрабатывать. Например, если «Режим работы входа» задан «На замыкание», то активным уровнем будет считаться состояние низкого уровня на входе. (По умолчанию «На замыкание»).

Изначальное состояние входа определяет в каком состоянии должен находиться вход при взятии его на охрану. Активным уровнем будет считаться уровень на входе инверсный начальному. (По умолчанию «Разомкнут»).

Время усреднения входного сигнала задается для исключения влияния переходного процесса при изменении состояния на входе, так называемый дребезг контактов. Обычно значение данного параметра находится в пределах от 100 до 500 мс. (По умолчанию 100 мс).

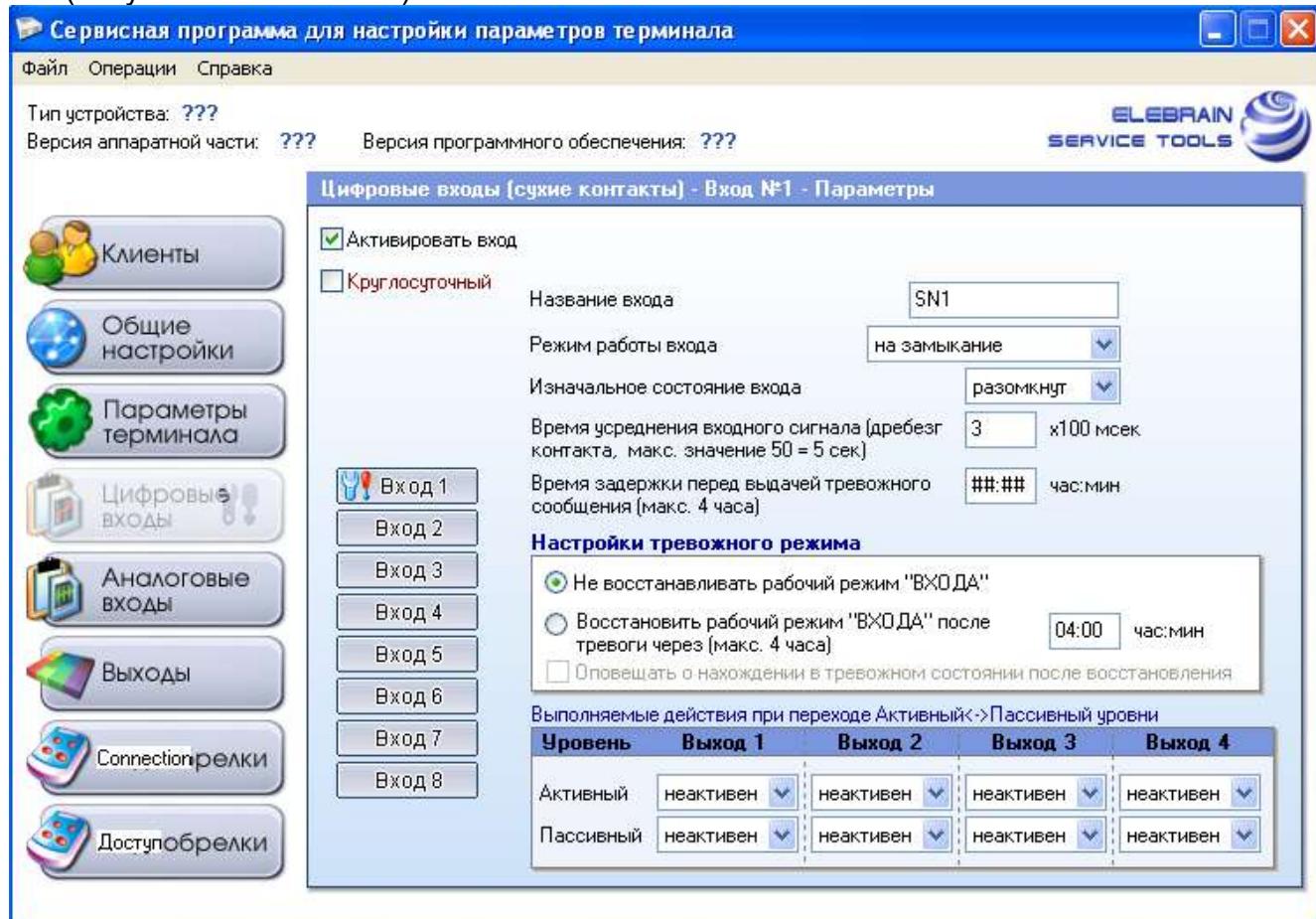


Рисунок 10. Окно настройки цифровых входов терминала.

Время задержки перед выдачей тревожного сообщения дает возможность пользователю системы снять терминал с охраны, до того как будет отправлено тревожное SMS-сообщение или активируется один из выходов, запрограммированный для данного входа. (По умолчанию ноль).

С помощью **настроек тревожного режима** можно гибко сконфигурировать обработку датчиков подключенных к данному входу. Когда состояние на входе соответствует активному уровню можно задать несколько режимов обработки:



- если задан «Не восстанавливать рабочий режим входа», это означает, что от входа пройдет только одно тревожное событие в охранную сессию, при переходе на входе в активный уровень;

- если задан «Восстанавливать рабочий режим входа после тревоги через интервал времени», это означает, что тревожное событие будет возникать каждый раз по завершению временного интервала, если состояние на входе будет соответствовать активному уровню;

- если задан «Восстанавливать рабочий режим входа после тревоги через интервал времени» и активирован параметр «Оповещать о тревожном состоянии после восстановления», это означает, что тревожное состояние будет возникать только тогда, когда после истечения временного интервала состояние на входе вновь измениться с изначального в активное. Т.е. датчик, подключенный к данному входу, после тревоги должен будет восстановиться.

(По умолчанию «Не восстанавливать рабочий режим входа»).

Каждому «Выходу» можно назначить **выполняемые действия при переходе «Активный» <-> «Пассивный» уровня на входе**, в соответствии с режимами работы «Выходов». (По умолчанию неактивен).

6.4.7. Объект настройки «Аналоговые входы»

Если вход активен, то разрешается обработка терминалом состояния на входе. Если данный параметр неактивен, то обработка состояния входа запрещена. (По умолчанию активен).

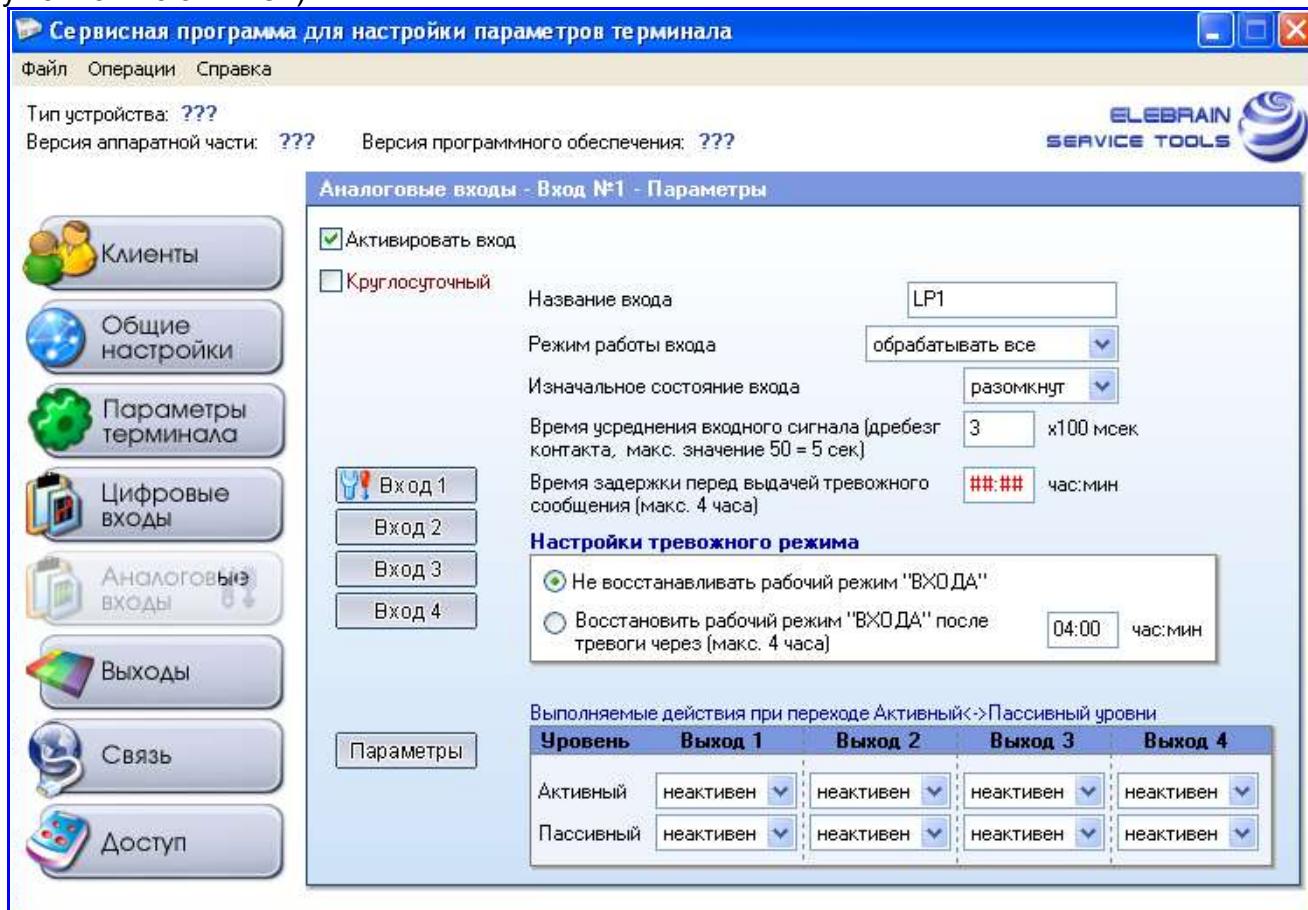


Рисунок 11. Окно настроек аналоговых входов терминала.

Если вход выбран – **круглосуточным** и вход **активен**, то обработка состояния на этом входе происходит не зависимо от состояния охраны терминала. (По умолчанию некруглосуточный).



Название входа – имя-псевдоним входа, используется в расширенном формате SMS-сообщения для более удобного восприятия клиентом входящей информации. В стандартном формате SMS-сообщения имя «Аналогового входа» соответствует «LP+номер входа». (По умолчанию «LP+номер входа»).

Режим работы входа указывает на то, какие состояния на входе необходимо обрабатывать. Например, если «Режим работы входа» задан «Обрабатывать все», то активным уровнем будет считаться значение на входе выше верхней границы или ниже нижней границы интервала пассивного состояния. (По умолчанию «Обрабатывать все»).

Изначальное состояние входа определяет в каком состоянии должен находиться вход при взятии его на охрану. Активным уровнем будет считаться уровень на входе инверсный начальному. (По умолчанию «Замкнут»).

Время усреднения входного сигнала задается для исключения влияния переходного процесса при изменении состояния на входе, так называемый дребезг контактов. Обычно значение данного параметра находится в пределах от 100 до 500 мс. (По умолчанию 100 мс).

Время задержки перед выдачей тревожного сообщения дает возможность пользователю системы снять терминал с охраны, до того как будет отправлено тревожное SMS-сообщение или активируется один из выходов, запрограммированный для данного входа. (По умолчанию ноль).

С помощью **настроек тревожного режима** можно гибко сконфигурировать обработку датчиков подключенных к данному входу. Когда состояние на входе соответствует активному уровню можно задать несколько режимов обработки:

- если задан «Не восстанавливать рабочий режим входа», это означает, что от входа пройдет только одно тревожное событие в охранную сессию, при переходе на входе в активный уровень;

- если задан «Восстанавливать рабочий режим входа после тревоги через интервал времени», это означает, что тревожное состояние будет возникать только тогда, когда после истечения временного интервала состояние на входе вновь измениться с изначального в активное. Т.е. датчик, подключенный к данному входу, после тревоги должен будет восстановиться.

(По умолчанию «Не восстанавливать рабочий режим входа»).

Каждому «Выходу» можно назначить **выполняемые действия при переходе «Активный» <-> «Пассивный» уровни на входе**, в соответствии с режимами работы «Выходов». (По умолчанию неактивен).

Основное отличие «Аналоговых входов» от «Цифровых входов», заключается в обработке сигнала поступающего на физический вход терминала. Если для «Цифрового входа» значения сигнала воспринимаются как два уровня: «Высокий» или «1» и «Низкий» или «0», то в обработке «Аналогового входа» используются все значения диапазона изменения входной величины. Текущие значение входной величины, а также значения уровней для обработки «Аналоговых входов», можно увидеть нажав кнопку «Параметры».

Внимание! Отображаемые в окне значения имеют размерность условных единиц, где значение 0=0 Вольтам подаваемым на аналоговый вход, а значение 255=3,3 Вольтам. Для подключения к аналоговому входу датчиков с диапазоном выходных напряжений в 12 или 24 Вольта необходимо использовать резистивный делитель напряжения. Для использования аналоговых входов терминала в качестве измерительно-сигнализирующей аппаратуры необходимо после подключения резистивного делителя откалибровать терминал, сопоставляя значения подаваемого напряжения и значения условных единиц отображаемых в этот момент в окне параметров аналоговых входов терминала. После этого можно составить таблицу



пересчета значений среды (температуры, давления, концентрации) в значения у.е., которые будет передавать терминал.

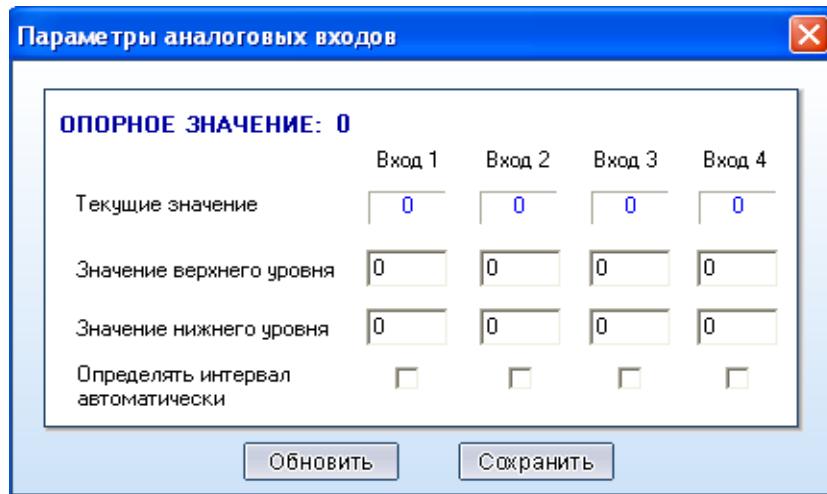


Рисунок 12. Окно параметров Аналоговых Входов Терминала.

Процедуру калибровки и сопоставления можно пропустить, если необходимо только контролировать отклонения напряжения на охранном шлейфе выше или ниже чем на 30% от напряжения заданного нормальным.

В окне «Параметры аналоговых входов» отражены следующие параметры:

Опорное значение – этот параметр отображает значение, которое используется для вычисления уровней, если активирован параметр «Определять интервал автоматически».

Текущие значение отображает значение величины, поступающие на аналоговый вход терминала.

Значение верхнего уровня – используется для задания верхней границы интервала пассивного состояния. Используется, если параметр «Определять интервал автоматически» неактивен.

Значение нижнего уровня – используется для задания нижней границы интервала пассивного состояния. Используется, если параметр «Определять интервал автоматически» неактивен.

Если активен параметр **определять интервал автоматически**, то значение нижней границы рассчитывается, как 30% от «Опорного значения», а значение верхней границы рассчитывается, как 70% от «Опорного значения».

Для отображения актуальных (текущих) данных в окне «Параметры аналоговых входов» необходимо нажать кнопку «Обновить».

Для внесения изменений значений параметров аналоговых вход в профильную конфигурацию необходимо нажать кнопку «Сохранить». Для выхода из окна «Параметры аналоговых входов», без изменения значений, нажмите крестик в правом верхнем углу окна.

6.4.8. Объект настройки «Выходы терминала»

Для выполнения каких либо действий над «Выходом» необходимо его **активировать**. (По умолчанию активен).

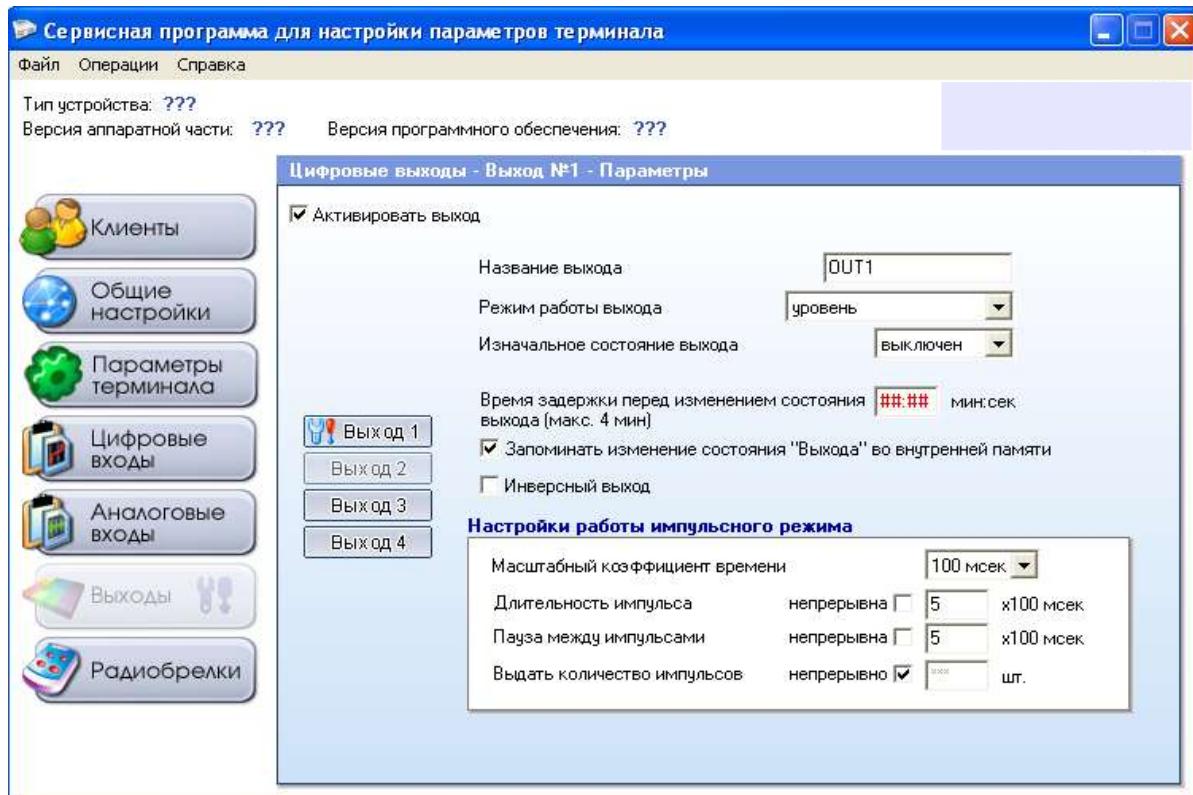


Рисунок 13. Окно настроек Выходов Терминала

В параметре название выхода можно задать имя-псевдоним, используется при входящем SMS-сообщении для управления «Выходом» или при отправки статусного SMS-сообщения в расширенном формате. (По умолчанию «OUT+номер выхода»).

Режим работы выхода может быть:

- «Уровень» (установлен по умолчанию) – состояние выхода соответствует заданному уровню и не изменяется во времени;
- «Импульсный» – состояние на физическом выходе терминала изменяется соответственно заданным настройкам работы выхода в импульсном режиме.

Изначальное состояние выхода – определяет в каком состоянии должен находиться выход после запуска терминала. (По умолчанию «Выкл»).

Время задержки перед изменением состояния выхода определяет задержку между командой управления выходом и изменением состоянием выхода, заданным командой управления. Например, если начальный режим работы был «Уровень» и командой управления задается «Импульсный», то импульсы на выходе появятся после истечения интервала времени задержки. (По умолчанию ноль).

Если активен параметр **запоминать изменение состояния выхода во внутренней памяти**, то все настройки, в том числе текущие состояния на выходе и режим, будут сохранены при пропаже питания и восстановлены после следующего запуска терминала. (По умолчанию активен).

Параметр **инверсный выход** задает режим работы выхода в противоположном логическом состоянии. (По умолчанию неактивен).

Настройкой работы импульсного режима можно задать значения следующих параметров:

- **Масштабный коэффициент времени** используется для изменения периода импульсов. (По умолчанию 100 мсек.).
- **Длительность импульса** задает продолжительность положительной части импульса, соответствующей состоянию «Включен». Если «Длительность



импульса» задана «Непрерывна», то у импульса будет всего один фронт и возврата в исходное состояние не произойдет. (По умолчанию 5 у.е.).

- **Пауза между импульсами** задает продолжительность паузы между положительными частями импульса, соответствует состоянию «Выключен». Если «Пауза между импульсами» задана как «Непрерывно», то будет сформирован всего один импульс (удобно для управления электромагнитными замками).
- Параметр **выдать количество импульсов** – определяет количество импульсов после вывода которых режим работы «Выхода» автоматически становится «Уровень». (По умолчанию бесконечность).

6.4.9. Объект настройки «Параметры Связи»

Для корректной работы терминала по GPRS каналу необходимо настроить ряд параметров подключения зависящих от конкретной компании-оператора сотовой связи.

Вид соединения для передачи сообщений – определяет канал связи для надежного оповещения клиентов, осуществляющих мониторинг данного объекта. Использование только канала SMS наиболее надежный и быстрый способ оповещения, однако и наиболее дорогостоящий и как следствие менее информативный и гибкий.

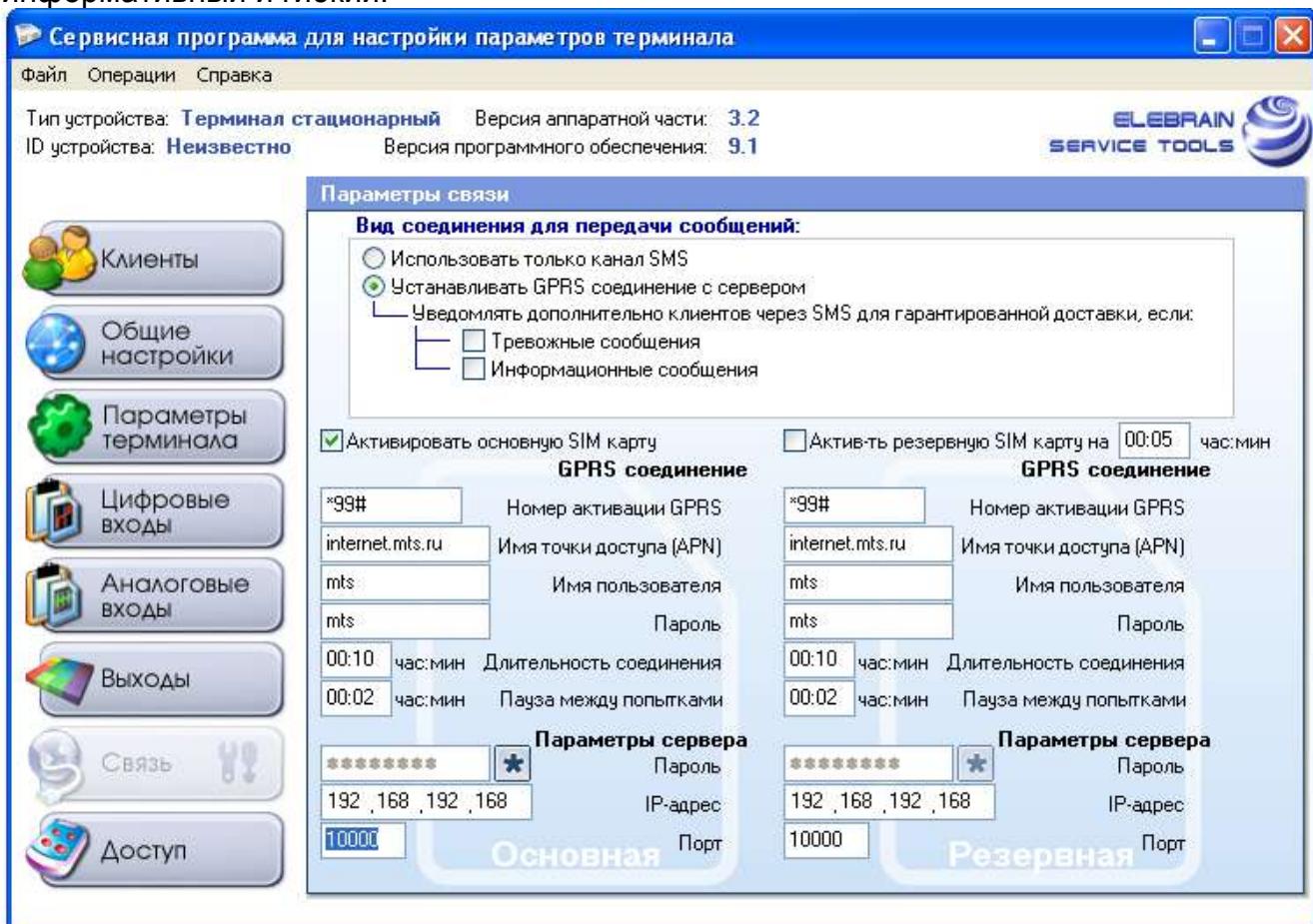


Рисунок 14. Окно настроек параметров связи

Комбинированное оповещение через GPRS канал с дублированием по SMS тревожных сообщений сочетает надежность и быстроту доставки по SMS сообщений высокого приоритета и низкой частоты с дешевизной и гибкостью управления устройством и контроля его состояния через GPRS канал. Для этого необходимо



отметить пункт «Устанавливать GPRS соединение с сервером» и подпункт «Тревожные Сообщения» в разделе «Уведомлять дополнительно клиентов через SMS...».

Пункты активации основной и резервной SIM карты определяют будет работать терминал в режиме резервирования канала связи или в режиме единственного канала связи. Не рекомендуется злоупотреблять переключением SIM-карт без реальной потребности в этом – частые перезагрузки SIM-карт могут негативно отразиться на их сроке службы. Процедура переключения между основной и резервными SIM-картами описана в приложении С.

Параметр «**Активировать Резервную SIM-карту на:**» определяет период времени, после которого работающий на резервной SIM карте терминал будет осуществлять попытки перехода на основную SIM карту. Минимальное значение – 5 минут, максимальное – 4 часа.

Непосредственно параметры соединения с сервером (ПК с установленным ПО Диспетчерского Центра SlyCenter) разделены на две группы для каждой SIM-карты:

Первая группа параметров определяет параметры транспортировки сообщений до сервера и определяются компанией-оператором сотовой связи выпустившей данную SIM-карту. **Номер активации GPRS, имя точки доступа, имя пользователя и пароль** необходимо запросить у оператора сотовой связи. Данная информация является открытой и ее могут предоставить как специалисты техподдержки, так и в автоматическом режиме в справочной службе. При отсутствии номера активации GPRS в справочной информации от ОпСоСа, можно оставить его по умолчанию, но при этом необходимо убедится, что услуга передачи данных по GPRS активирована для данной SIM карты.

Кроме того, в этой группе указано **время поддержания GPRS сессии** и **длительность пауз между попытками установления соединения**. Время GPRS сессии желательно определить исходя из среднего времени отклика ДЦ (если по регламенту работы оператор должен в ответ на событие послать команду). Однако, увеличивая длительность сессии, не стоит забывать, что данное ограничение служит для гарантированных доставок SMS команд от зарегистрированных клиентов терминала (в процессе установленной сессии терминал не может обрабатывать SMS команды).

Длительность пауз между семью попытками соединения необходимо определять исходя из возможного количества сообщений, которые могут накопиться в терминале и которые будут отправлены в паузе между попытками установления GPRS подключения. В случае, если не выбран параметр дублирования GPRS сообщений, сообщениями SMS, то время между паузами можно уменьшить.

Вторая группа параметров позволяет успешно пройти авторизацию и подключение непосредственно к серверу Диспетчерского центра. Эта группа параметров определяется администратором сервера при инсталляции и настройке ПО SlyCenter.

Пароль необходим для невозможности подмены терминала сотовым телефоном злоумышленника с перепрошитым IMEI с целью формирования ложных срабатываний или наоборот, комплексной работы с «глушилкой», для отправки сигналов жизни.

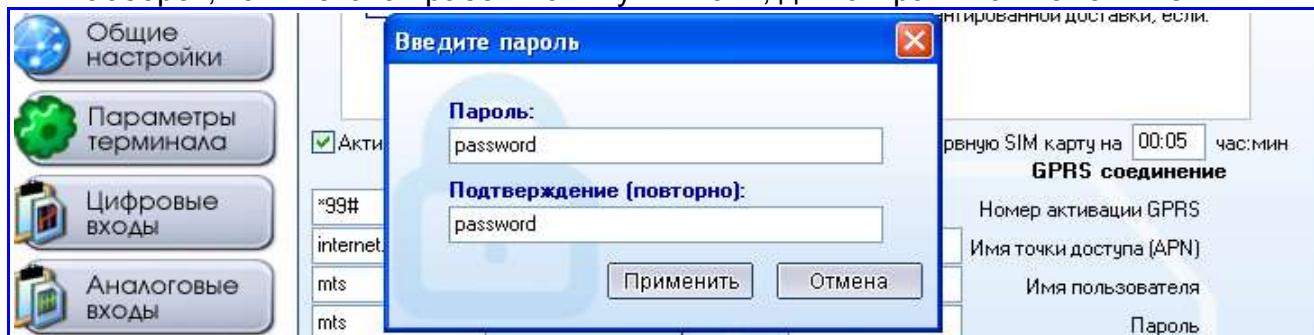


Рисунок 15. Окно настроек параметров связи. Окно пароля на подключение



Пароль закрывается знаком * с тем, чтобы невозможно было его считать. В случае изменения пароля на сервере пароль можно изменить, для чего ввести его дважды в дополнительном окне ввода пароля.

После переключения на использование резервной SIM-карты терминалом на сервер будет отправлено соответствующее сообщение (статус: информационное).

6.4.10. Объект настройки «Управление Доступом»

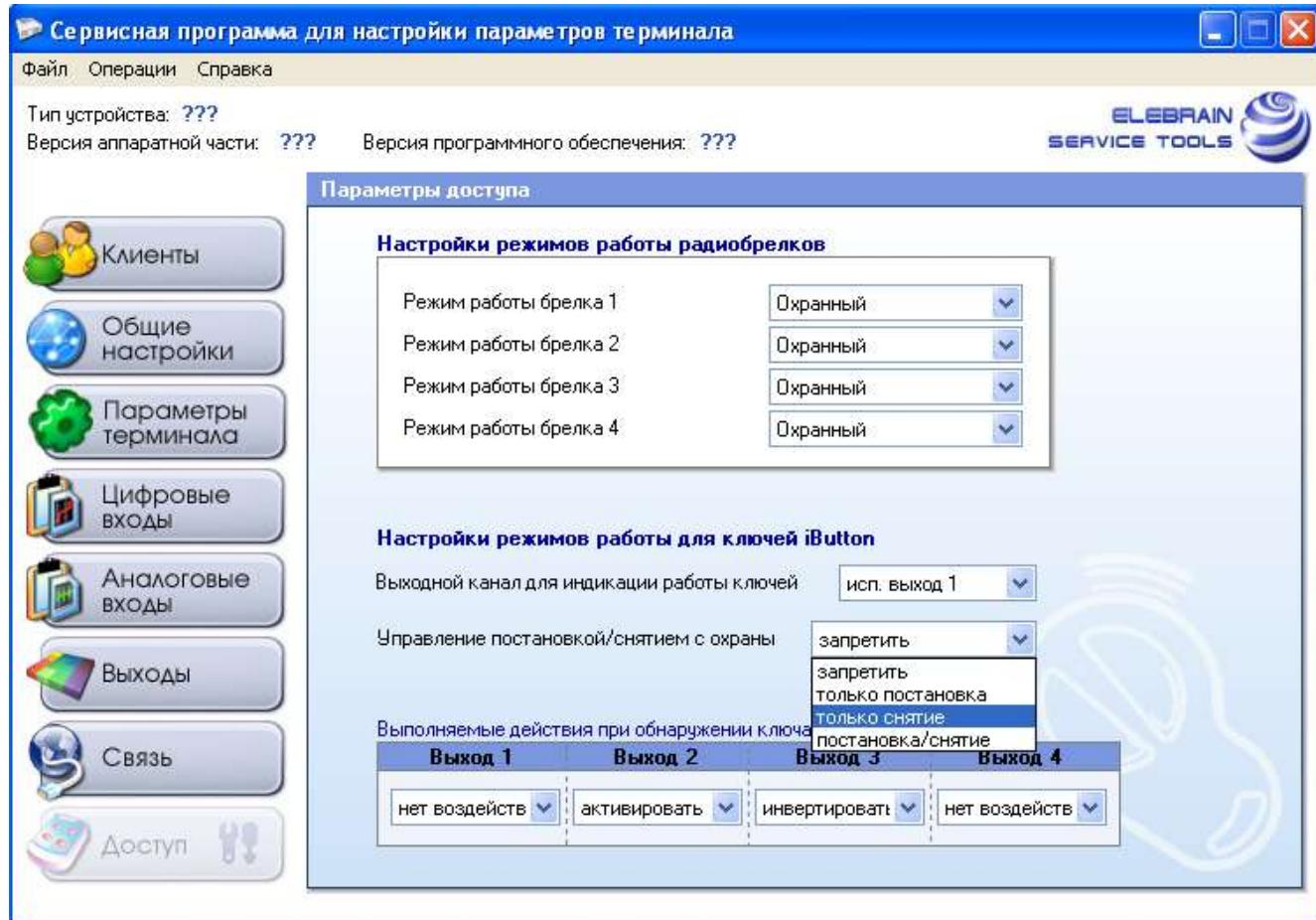


Рисунок 16. Окно настроек параметров доступа

Настройка режимов работы радиобрелков

Для каждого радиобрелка можно задать свой режим работы:

- «Охранный» - определяет реакцию на брелок как: кнопка №1 – постановку терминала на охрану, кнопка №2 – снятие терминала с охраны, кнопка №3 – нет реакции, кнопка №4 – нет реакции.

- «Тревожный» - определяет реакцию на нажатие любой кнопки, как тревожное событие («тревожная кнопка»), с последующей отправкой терминала тревожного SMS-сообщения, действий над «Выходами» не происходит.

- «Охранно-тревожный» - определяет реакцию на брелок как: кнопка №1 – постановку терминала на охрану, кнопка №2 – снятие терминала с охраны, кнопка №3 – «тревожная кнопка», кнопка №4 – «тревожная кнопка».

В режиме тревожной кнопки при срабатывании брелка терминал генерирует «тихую тревогу» без какой-либо индикации на своем корпусе или выходах, но с отправкой тревожного сообщения на ПЦН.

(По умолчанию «Охранный»).



Настройка режимов работы для ключей iButton (TouchMemory).

Данные параметры определяют реакцию терминала на обнаружение на контакторе ТМ электронного ключа пользователя с кодом-идентификатором занесенным в базу электронных ключей пользователей терминала.

Ключи с кодами-идентификаторами находящиеся в базе ключей сотрудников ЧОП/ГБР не имеют возможности как-либо влиять на состояние терминала и режимы его работы, а потому данные настройки не влияют на них.

Настроив Выходной канал для индикации работы ключей на индикацию через один из четырех выходов терминала можно подключить данный выход к световому или звуковому индикатору контактора ТМ или иному световому или звуковому индикатору. В случае срабатывания контроллера данный выход будет формировать либо одиночный импульс (при успешной аутентификации электронного ключа пользователя), последовательный набор импульсов в течение определенного промежутка времени (запуск процедуры изменения базы электронных ключей с помощью MasterKey), либо одиночный импульс увеличенной длительности (при добавлении или удалении кода-идентификатора ключа пользователя).

Электронные ключи пользователей могут оказывать влияние на состояние охраны, а могут только управлять состоянием выходов (применяется для разграничения доступа в помещения оборудованные электрозамками в течение рабочего времени) не оказывая влияния на процедуру начала/завершения охранной сессии. Выбрав для параметра «Управление постановкой/снятием с охраны» значение «запретить» вы создадите ситуацию, когда приложение электронного ключа к контактору не приведет к изменению состояния охраны. Выбрав значение только постановка вы можете разрешить вашим пользователям электронных ключей только ставить на охрану Ваш объект и управлять выходами, но при этом снять с охраны терминал они не смогут. Аналогичная ситуация со значением «только снятие» - пользователи смогут снять с охраны терминал электронным ключом, но не смогут его поставить. Значение «постановка/снятие» создаст конфигурацию, когда при каждом считывании электронного ключа будет происходить смена состояния терминала – либо начало его охранной сессии, либо ее завершение.

Для каждого выхода терминала можно запрограммировать реакцию на считывание терминалом кода-идентификатора электронного ключа пользователя. Значение «нет воздействия» обозначает, что данный вход не будет реагировать ни на какие электронные ключи. Значение «активировать» обозначает, что при приложении авторизованного ключа к контактору будет происходить перевод данного выхода в активное состояние, независимо от того, в каком состоянии он был перед этим. Конкретные действия на выходе, соответствующие активному состоянию настраиваются в разделе «Выходы». Значение «инвертировать» обозначает, что при приложении авторизованного ключа к контактору будет происходить изменение состояния выхода на противоположное: в случае если выход был в активном состоянии, то он будет переведен в «изначальное», если он был в «изначальном состоянии», то он будет переведен в активное.

Пример использования: Настроить активное состояние выхода на формирование одиночного импульса с «непрерывной» паузой между ними. Настроить значение «активировать электронным ключом» для данного выхода. Подсоединить данный выход к электромагнитному замку так, чтобы при формировании импульса происходило его открытие. В данном случае каждое приложение электронного ключа к контактору будет производить открытие двери.



7. Подключение устройства

7.1. Назначение выводов разъема

Назначение выводов терминала для самостоятельного обжима или пайки разъема.

Таблица 4

№	Состояние	Назначение вывода, описание
1	Выход	Открытый Коллектор №1 (Цифровой выход)
2	Выход	Открытый Коллектор №2 (Цифровой выход)
3	Вход	Шлейф связи безадресный №4 / Аналоговый вход №4
4	Вход	Шлейф связи безадресный №3 / Аналоговый вход №3
5	Вход	Шлейф связи безадресный №2 / Аналоговый вход №2
6	Вход	Шлейф связи безадресный №1 / Аналоговый вход №1
7	Вход	Цифровой вход №1
8	Вход	Цифровой вход №2
9	Вход	Цифровой вход №3
10	Вход	Цифровой вход №4 / Обучение MasterKey (группы «ГБР/ обслуживающий персонал»)
11	Вход	Цифровой вход №5 / Обучение MasterKey (группы «пользователи»)
12	Вход	Цифровой вход №6 / Обучение радиобрелков
13	Вход	Цифровой вход №7
14	Выход	Реле № 2 Нормально Открытый
15	Выход	Реле № 2 общий
16	Выход	Реле № 2 Нормально Замкнутый
17	Выход	Реле № 1 Нормально Открытый
18	Выход	Реле № 1 общий
19	Выход	Реле № 1 Нормально Замкнутый
20	Выход	VCC +12 В; 0,5 А
21	Общий	Общий (земля)
22	Общий	VDC +5 В
23	Общий	Общий (земля)
24	Вход	Электронный Ключ (Touch Memory)
25	Вход	Цифровой вход №8



7.2. Общая схема подключения.

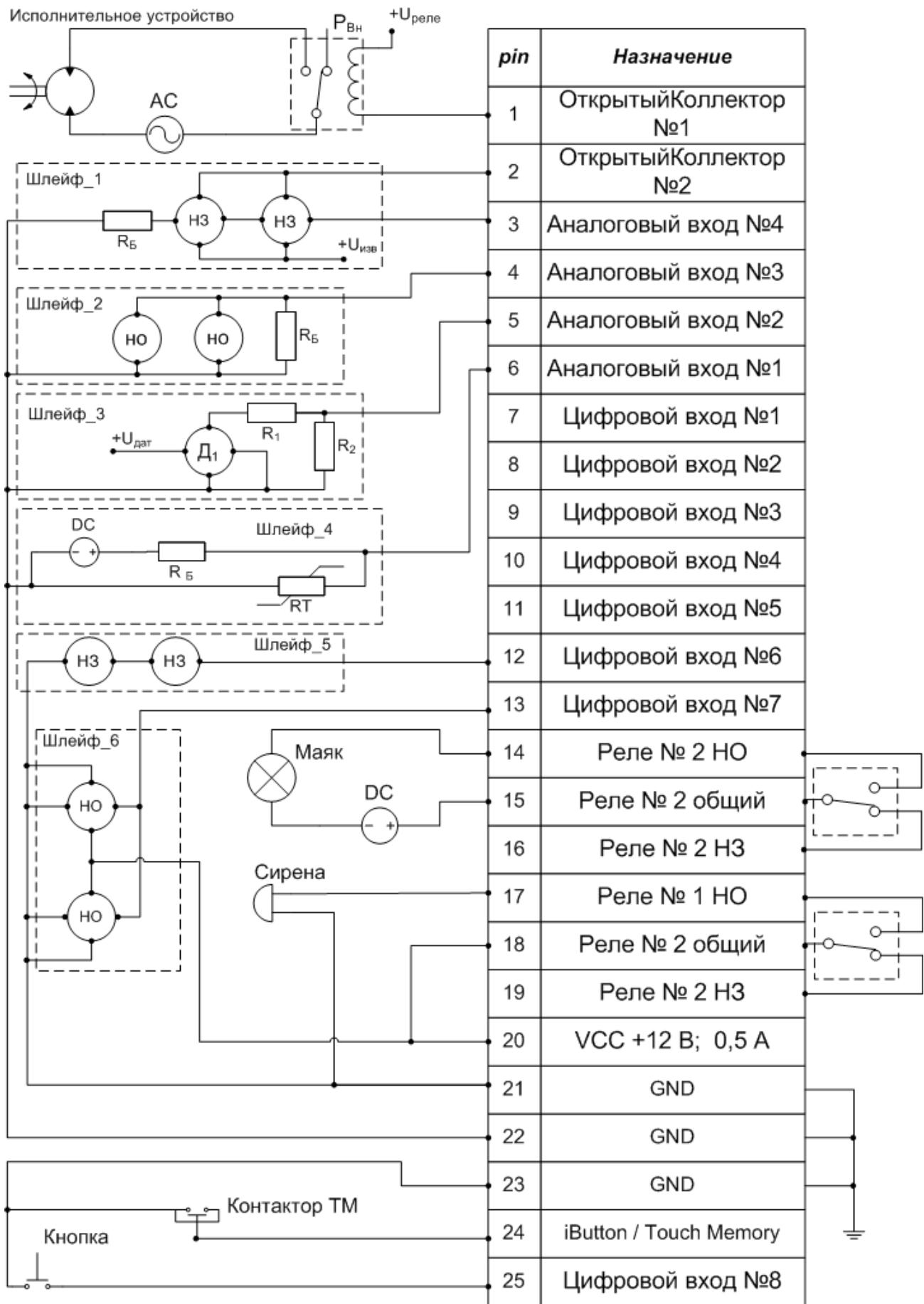


Рисунок 17. Общая схема подключения.



На общей схеме подключения:

Исполнительное устройство – любое устройство оказывающее воздействие на среду наблюдаемого объекта. Это может быть электромотор, вытяжка, тепловая пушка или завеса, пиропатрон. На данной схеме показано включение этого устройства через внешнее реле $P_{вн}$. При этом параметр $U_{реле}$ выбирается в соответствии с характеристиками реле, а параметры источника питания (на схеме **AC**) в соответствии с характеристиками исполнительного устройства. Выход ОК терминала необходимо настроить в соответствии с особенностями работы данного устройства и параметров реле: возможно настройка включения устройства постоянным уровнем, возможно включение его на определенный промежуток времени с последующим отключением, возможно включение его определенными периодами.

Шлейф_1

Датчики НЗ – Датчики типа сухой контакт находящиеся в нормально-замкнутом состоянии. R_b в подобной цепи обычно равен 1 кОм. Датчики одного периметра соединяются в цепь последовательно. В данном примере подключения изображены **активные датчики** требующие для работы подведения питания. Питание к ним подведено от выхода **OK №2**. Сделано это для того, чтобы можно было подавать питание на датчики этого шлейфа только в период охранной сессии. Для этого необходимо сконфигурировать цифровой выход **OK №2** на включение с формированием постоянного уровня при постановке терминала на охрану. После постановки на охрану цепь питания извещателей $U_{изв}$ будет замкнута на землю, через выход ОК терминала.

Внимание. Все источники питания включенные в цепи выходов типа Открытый Коллектор должны иметь общую землю. Если устройства, включаемые в эти цепи, требуют различные номиналы напряжений рекомендуется использовать блоки питания с различными номиналами, но не использовать независимые блоки питания на разные номиналы!

Шлейф_2

Датчики НО - Датчики типа сухой контакт находящиеся в нормально-открытом состоянии. R_b в подобной цепи обычно равен 1 кОм. Датчики одного периметра соединяются друг с другом и балансным резистором в цепь параллельно.

Шлейф_3

Подключение активного аналогового датчика/измерительного прибора. Д1 – датчик формирующий на своем выходе конкретные значения напряжения пропорционально изменению контролируемого им физического параметра. В случае если пределы выходных напряжений не превышают 3,3 В, можно не использовать резистивный делитель ($R_1; R_2$), во всех остальных случаях необходимо подбирать значения сопротивлений так, чтобы максимальное значение напряжения на входе терминала ТСИ-03 не превышало 3,3 В.

Шлейф_4

RT – датчик температуры, изменяющий свое сопротивление пропорционально изменению температуры контролируемой среды. R_b - балластное сопротивление, служащее для приведения параметров тока и напряжения на аналоговом входе терминала в соответствие с рабочим диапазоном. Вместо датчика температуры можно использовать любой другой датчик изменяющий свое сопротивление пропорционально изменению определенного параметра контролируемой среды. **DC** – источник питания постоянного тока.



В случае, когда датчик самостоятельно генерирует на своих выходных контактах изменение напряжения или тока, то необходимо вместо R_T и R_b включить в схему два резистора R_{d1} и R_{d2} , с таким значением сопротивлений, чтобы максимальное значение напряжения на входе терминала не превышало значение 3,3 В.

Маяк – оповещатель световой имеющий независимое питание. Вместо маяка может стоять оповещатель комбинированный светозвуковой, электрозамок, тепловая пушка, система пожаротушения и любое другое устройство с независимым электропитанием. При включении данного выхода происходит коммутация цепи питания внутренним реле терминала.

Сирена – оповещатель звуковой, питающийся от внутреннего питания VCC +12 В терминала. может использоваться и другие исполнительные устройства с максимальным потребляемым током не более 0,5 А.

Контактор ТМ – Контактная площадка для электронных ключей TouchMemory.

Кнопка – механическая кнопка начала/завершения охранной сессии. В зависимости от конфигурации терминала кнопка может быть заменена на тумблер или переключатель.



7.3. Подключение Питания терминала ТСИ-03.

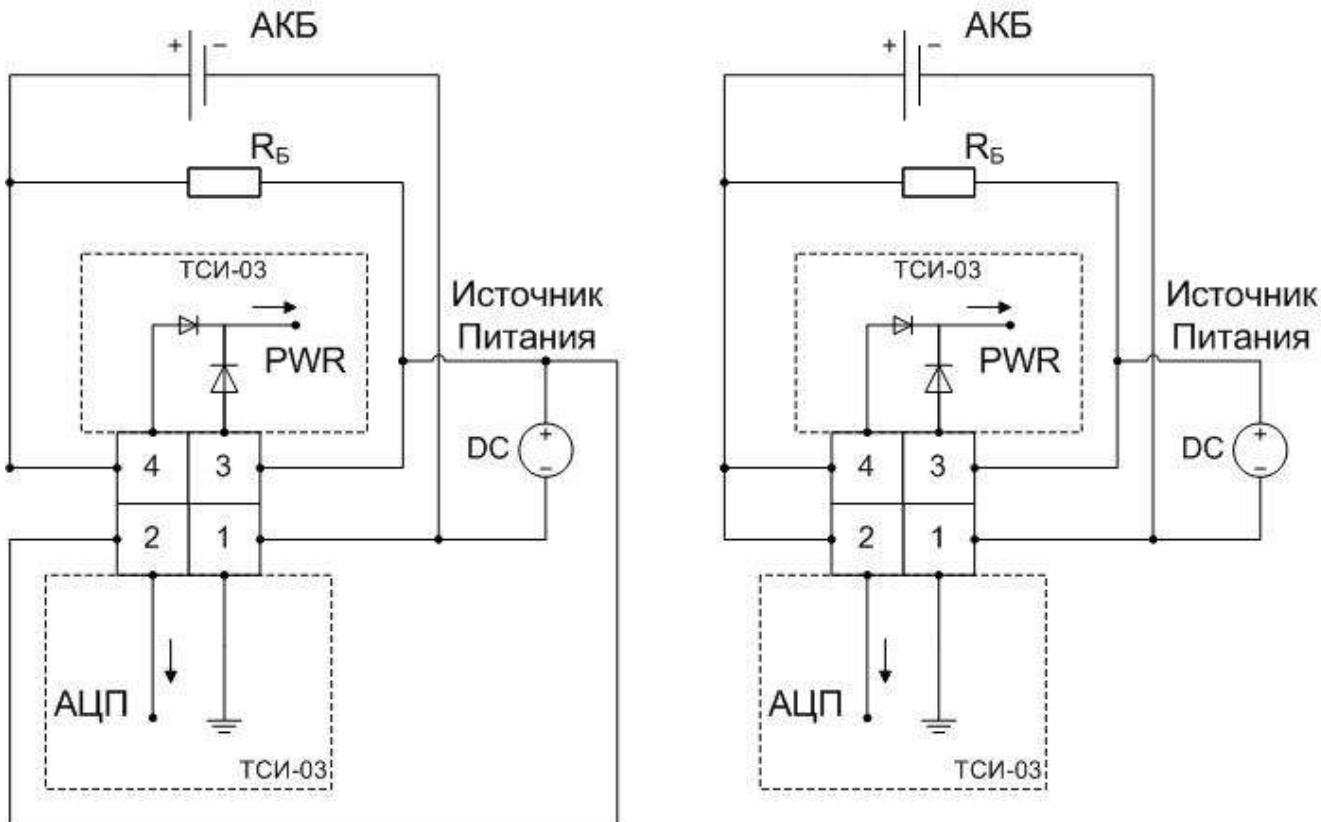


Рисунок 18. Подключение питания

На схеме:

Источник Питания – Блок Электропитания постоянного тока номиналом 12 В. (В данной схеме не допускается подключения источников питания другого номинала)

АКБ – Аккумуляторная батарея номиналом 12 В. Подключенная по данной схеме осуществляет одновременно и резервирование терминала ТСИ-03 и собственный подзаряд от Источника Питания через мощный низкоомный резистор R_B . Номинал резистора определяется емкостью конкретного аккумулятора, для аккумулятора емкостью 1,3 Ah рекомендуется выбирать резистор номиналом 100 Ом, мощностью порядка 5 Вт.

АЦП – Аналоговый вход процессора ТСИ-03. Осуществляет контроль параметров электропитания. В зависимости от коммутации контролирует либо уровень заряда аккумулятора (рисунок справа), либо наличие и уровень напряжения на Источнике Питания (рисунок слева).

Пины 3 и 4 разъема питания соединены через два диода, по схеме обеспечивающей запирание при наличии напряжения 12 и более Вольт на источнике питания и препятствующие разряду аккумулятора через цепи источника питания.



7.4. Подключение GSM-антенны

GSM-антенну необходимо подключать при выключенном питании терминала к ВЧ разъему X1. Антenna должна располагаться в скрытом месте, в котором она осуществляла бы уверенный прием сигнала сотовой связи. Капитальный монтаж GSM-антенны должен быть осуществлен только после подтверждения надежного приема сигнала в месте предполагаемой установки!

8. Внешний вид устройства



Рисунок 19. Внешний вид устройства ТСИ-03.



9. Внешний вид и подключение элементов расширения

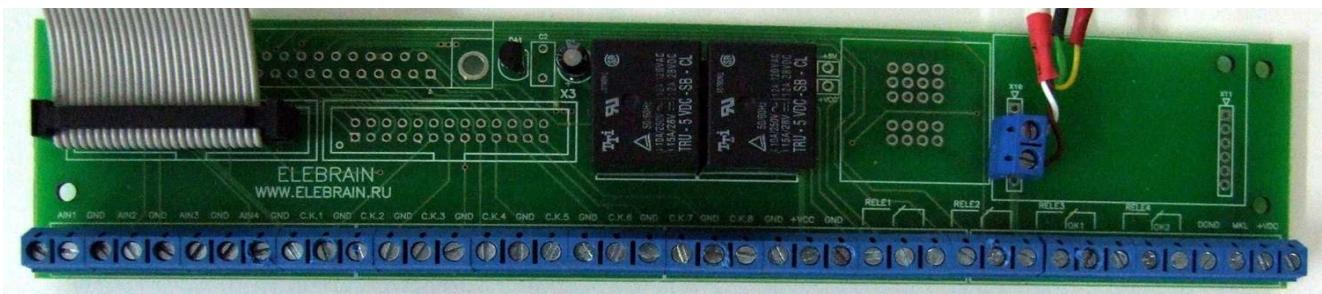


Рисунок 20. Монтажная плата МП-5.

Условные обозначения и сокращения используемые для обозначения контактных зажимов монтажной платы МП-5:

Таблица 5

Наименование	Назначение
AIN1...AIN4	Сигнальный («+») контакт аналогового входа/входа ШСБ
CK1...CK8	Сигнальный («+») контакт цифрового входа типа «сухой контакт»
+VCC	Выход питания для подключения датчиков и исполнительных устройств питающихся от 12 В
GND	Общий (земля), минус.
Rele1...Rele4	Релейный выходы терминала 1...4
DGND	Земля, для подключения контактора TouchMemory
MKL	Сигнальный контакт для подключения контактора TouchMemory
+VDC	Питание +5V для устройств, подключаемых к MKL

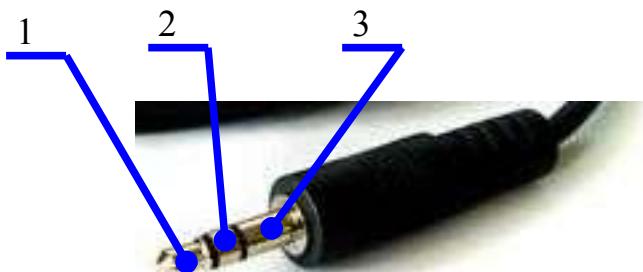


Рисунок 21. Разъем активного микрофона типа Шорох

На рисунке распайка разъема:

1. +5 V (питание микрофона)
2. Mic (сигнал)
3. GND (общий)



10. Основные технические характеристики

Электрические характеристики

Таблица 6

Параметры электропитания	
Допустимое напряжение питания, В	8-32
Потребляемый ток (для напряжения питания 12,5 В), мА	
• в ждущем режиме	50
• в режиме голосового дозвона и соединения	1000
Параметры входных линий	
Количество входных шлейфов, шт.	8
Входное сопротивление, не менее, кОм	2
Ток потребления входных цепей, не более, мА	10
Минимально необходимое время для фиксации тревожного сигнала, мс	100-300
Параметры выходных линий	
Количество выходов управления исполнительными устройствами, шт.	4
Тип выхода управления исполнительными устройствами	2 Открытый сток + 2 перекидных реле
Максимальный допустимый ток нагрузки по цепи управления исполнительными устройствами, А	1 А (открытый сток), 3А (реле).
Максимальное допустимое напряжение в цепи управления исполнительными устройствами, В	24
Параметры измерения напряжения источника питания	
Максимальное измеряемое напряжение, В	32
Точность, не хуже, В	0,2

Параметры внутреннего запоминающего устройства

Таблица 7

Тип памяти	Энергонезависимая
Время хранения данных при отсутствии питания, не менее, лет	10
Тип организации	Кольцевой буфер

Система связи

Таблица 8

Тип системы связи	GSM-900/1800
Канал для передачи данных	SMS, GPRS, EDGE
Удалённое акустическое прослушивание	Голосовой канал
Максимальное количество SMS абонентов	8
Максимальное количество абонентов для акустического оповещения и удалённого прослушивания	8

Массогабаритные параметры, устойчивость к внешним воздействиям

Таблица 9

Габаритные размеры системного блока, мм	145x95x35
Масса системного блока, кг	0,25
Температура хранения, °C	-40... +85



Продолжение таблицы 9

Рабочая температура, °C	-15... +50
Повышенная влажность при 35°C, %	95
Максимально допустимая перегрузка при ударах, г	5



Приложение А. Пояснения к тексту.

1 прибор приемо-контрольный - электротехническое устройство предназначено для контроля состояния выходов датчиков, подсоединеных к его входным шлейфам, обработке этих состояний по определенному установленному алгоритму, формированию в соответствии с охранным алгоритмом соответствующих (тревожных, информационных) сигналов и отправке этих сигналов на свои выходы, для включения исполнительных устройств, либо в линии связи, для оповещения ответственных за контроль состояния объекта.

2 датчики – электротехнические устройства, преобразующие изменения состояния контролируемого ими объекта (помещения, двери, звукового фона или температурного фона) в определенного вида электрический сигнал (последовательность импульсов, падение или наоборот всплеск напряжения) на своем выходе, пригодный для дальнейшей обработки приборами приемо-контрольными.

3 законченные системы – под законченными системами в данном контексте понимаются готовые комплексы, состоящие из датчиков и приборов приемо-контрольных. В таком случае к входным шлейфам терминала подключаются не выходы датчиков, а выходы приборов приемо-контрольных. При подобной схеме подключения снижается детализация приходящих сообщений, но появляется возможность расширения количества и номенклатуры подключаемых устройств. Таким образом, например, можно подключить комплексы радиодатчиков работающих в связке с приемо-передающей контрольной панелью.

4 параметры выходного (тревожного) сигнала – в зависимости от типа устройства, его выходной сигнал может иметь вид (для входов терминала типа «сухой контакт»): подъема напряжения («левый фронт»), падения напряжения («правый фронт») или кратковременных импульсов напряжения.

5 цифровые входы – входы терминала типа «сухой контакт» - рассчитаны на контроль резких изменений напряжений в контролируемой электрической цепи. Не привязаны к конкретным значениям напряжений.

6 аналоговые входы – Входы терминала считающие абсолютное значение напряжения и преобразующие его в цифровой вид для дальнейшей обработки. Для аналоговых входов терминала тревожным сигналом будет достижение напряжением на входе определенного значения за пределами (выше или ниже) установленной при настройке «рабочего» диапазона напряжений. Требуют предварительной настройки и подключения дополнительных резисторов для приведения параметров напряжения в линии к диапазону безопасной работы аналоговых входов. **Подключение только квалифицированным персоналом!**

7 релейный канал управления – выходные контакты, коммутирующие или разрывающие, по команде с центрального процессора терминала, цепь питания исполнительного устройства.

8 исполнительные устройства - сирены, маяки, пиропатроны, электрозамки, тепловые пушки, вытяжки – устройства осуществляющие непосредственную резидентную автоматизированную защиту объекта.



9 пульт диспетчерского центра - представляет из себя Персональный компьютер (Минимальные системные требования Процессор - Celeron 1800 Mhz; ОЗУ 256Mb; Жесткий диск - 80 Gb) с подключенным к нему GSM-модемом и установленным ПО (SQLServer и ПО Client-Server ДЦ – поставляются отдельно).

10 тревожные сообщения – сообщения содержащие информацию о срабатывании конкретного датчика на охраняемом объекте поставленного под охрану или установленного на круглосуточный контроль состояния объекта.

11 информационные сообщения – сообщения обеспечивающие функционирование комплекса в нормальном режиме: периодические сообщения подтверждения работоспособности терминала («сигналы жизни»), сообщения о постановке/снятии объекта с охраны и т.п.

12 SMS (англ. Short Message Service — служба коротких сообщений) — это система, позволяющая посыпать и принимать текстовые сообщения при помощи сотового телефона или GSM-модема.

SMS сообщения, как правило, доставляются в течение нескольких секунд. Можно отправить сообщение на выключенный/находящийся вне зоны обслуживания телефон. Как только адресат выйдет на связь, он получит сообщение. Можно отправить сообщение абоненту, который в данный момент занят разговором. В отличие от голосового звонка сессию связи прервать практически невозможно, т.к. ее длительность составляет секунды. Кроме того, в отличие от голосового звонка, с помощью СМС происходит оповещение ВСЕХ ответственных за объект лиц за несоизмеримо более короткий период времени.

13 GPRS (англ. General Packet Radio Service — пакетная радиосвязь общего пользования) — надстройка над технологией мобильной связи GSM, осуществляющая пакетную передачу данных. GPRS позволяет пользователю мобильного телефона производить обмен данными с другими устройствами в сети GSM и с внешними сетями, в том числе Интернет. GPRS предполагает тарификацию по объему переданной/полученной информации, а не времени.

14 Контактная память (от [англ. Touch Memory](#) иногда встречается [англ. iButton](#)) — класс электронных устройств, имеющих двупроводный протокол обмена информацией с ними (1-Wire), и помещённых в стандартный металлический корпус (обычно имеющий вид «таблетки»).

Металлический корпус служит для защиты находящихся внутри микросхем.

Внутри может использоваться достаточно разнообразная электроника от однократно-записываемой и флэш-памяти, до всевозможных контроллеров, таймеров, датчиков температуры и т. п.

Устройство активизируется в момент контакта со считывателем. Операции чтения и записи осуществляются практически мгновенно во время контакта.

В простейшем случае это просто энергонезависимая память, размещаемая в металлическом корпусе.



Приложение Б. Специфические схемы подключения устройства.

Б.1. Защищенное подключение устройств с контактным выходом к цифровым входам устройства.

Сфера применения. В случае если злоумышленник имеет кратковременный безнадзорный доступ внутрь охраняемого помещения в момент когда оно снято с охраны (например, хозяева находятся на объекте), то имея опыт и знания принципов работы конкретных датчиков он может достаточно простым способом вывести их из строя. Так, например, определив, что на двери находится известный ему герконовый датчик, находящийся в нормально замкнутом состоянии при закрытой двери и размыкающий контакт при открытии двери, он может воткнуть в проводку идущую к этому датчику иглу или скрепку. На данную манипуляцию у него уйдет от одной до 3-х секунд. Обнаружив же датчик находящийся в нормально открытом состоянии и замыкающий контакты при возникновении тревожной ситуации (например, тревожная кнопка) он может карманными кусачиками перекусить этот шлейф. На данную операцию у него так же уйдет от 1 до 3-х секунд. Очевидно, что у опытного злоумышленника отвлечь хозяев на столь короткий промежуток времени не составит труда. Данный временной интервал можно увеличить «спрятав» шлейф сигнализации в кабель-канал или вмонтировав в стену. Однако при этом все равно остаются уязвимыми местастыка кабель-канала и датчика. Для того, чтобы поставить серьезный заслон злоумышленнику в этих уязвимых местах рекомендуется использовать данные четырехпроводные схему включения.

Под защищенным подключением подразумевается дополнение двухпроводной схемы подключения датчиков с контактным выходом до четырехпроводной схемы для предотвращения злонамеренного вывода из строя линий связи путем скрытого обрыва шлейфов связи с датчиками с нормально открытым состоянием (НО) и путем скрытого злонамеренного замыкания шлейфа связи с датчиками с нормально замкнутым состоянием (НЗ). Данная схема актуальна только для подключения к цифровым входам устройства. Аналоговые входы оценивают не процесс замыкания/размыкания контактов, а изменения сопротивления шлейфа с датчиком в определенных пределах. Аналоговый вход способен отличить обрыв связи с датчиком или короткое замыкание (КЗ) на шлейфе связи при корректном подключении внешнего сопротивления делителя напряжения без дополнительных мер.

Б.2. Принцип действия подключения.

В случае если злоумышленник пытается замкнуть шлейф нормально-замкнутого датчика подсоединеного к «Входу 2» на рисунке Б1 внедрением в него иглы или скрепки он также замкнет и сопроводительные провода шлейфа подсоединеного к Нормально Открытым «Входу 1». (концы сопроводительного шлейфа необходимо оставить заизолированными и ни к чему не подключать на стороне датчика). В результате данной попытки выведения из строя шлейфа «Вход 1» выдаст тревожное сообщение.

В случае же если злоумышленник пытается обрезать шлейф датчика подсоединеного к Нормально Открытым «Входу 2» на рисунке Б2, то он одновременно обрезает и сопроводительный шлейф от «Входа 1» находящийся в Нормально Замкнутом состоянии (концы сопроводительного шлейфа необходимо скрутить или спаять между собой на стороне датчика). В результате данной попытки выведения из строя шлейфа «Вход 1» выдаст тревожное сообщение.

Для подключения по защищенной схеме желательно использовать стандартный телефонный четырех проводной кабель (евро стандарт). Данный кабель имеет НТЦ «Элебрейн», г.Орел, 2008



удобную разноцветную индивидуальную изоляцию на каждый провод плюс прочную общую внешнюю изоляцию на все четыре провода.

Для эффективного противодействия злоумышленному выведению из строя шлейфа связи необходимо скрыть в корпусе датчика или под ним не только провода, непосредственно к нему подсоединяемые, но и провода сопроводительного шлейфа.

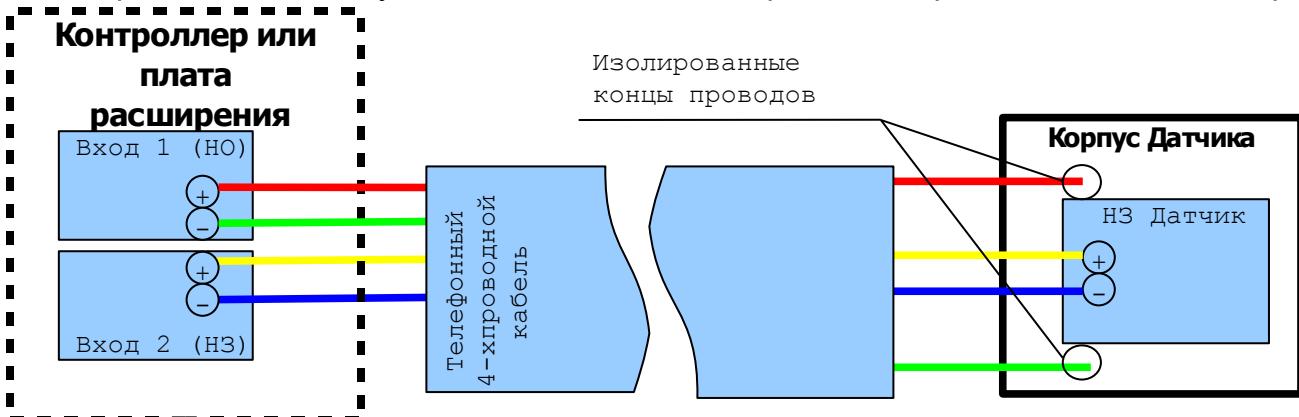


Рисунок Б1 – Защищенное подключение Нормально-Замкнутого Датчика к Цифровым входам устройства

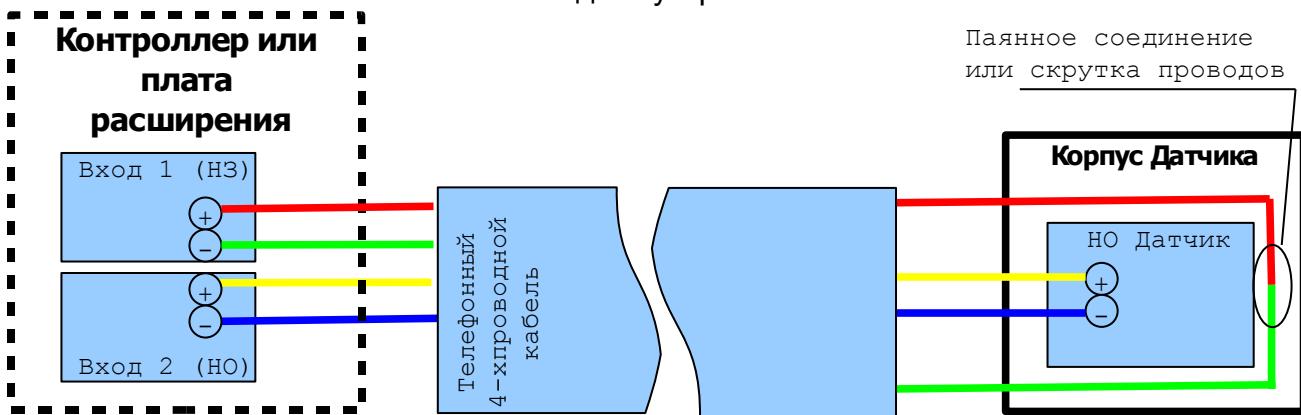


Рисунок Б2 – Защищенное подключение Нормально-Открытого Датчика Цифровым входам устройства

Б.3. Подключение датчиков с контактным выходом к аналоговым входам устройства.

НормальноЗамкнутые и НормальноРазомкнутые датчики типа «сухой контакт» можно подсоединять к Аналоговым Входам. При подключении можно объединять их в группы по назначению или расположению.

Нормально замкнутые датчики объединять в шлейф нужно последовательно друг с другом и с дополнительным сопротивлением (рекомендуется резистор со значением 1 кОм).

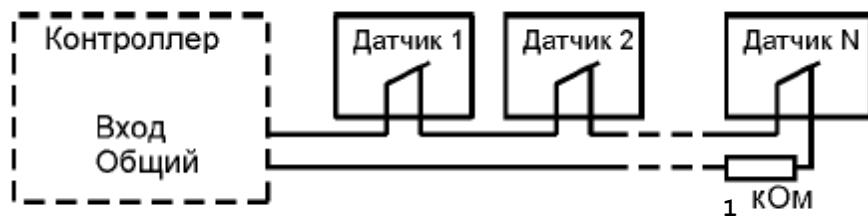


Рисунок Б3 – Подключение НормальноЗамкнутых Датчиков типа «Сухой Контакт».

Нормально Открытые датчики объединять в шлейф нужно параллельно друг с другом и с дополнительным сопротивлением (рекомендуется резистор со значением 1 кОм).

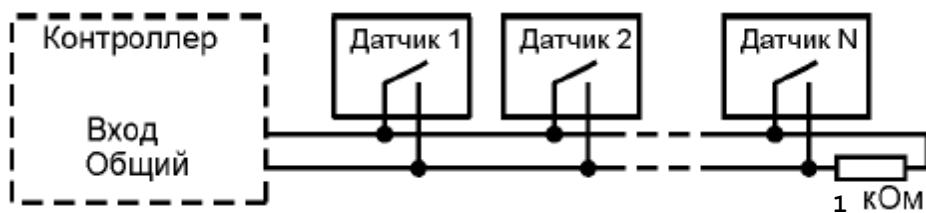


Рисунок Б4 – Подключение Нормально Открытых Датчиков типа «Сухой Контакт».

Внимание. Резистор является обязательной частью схемы подключения любых датчиков и должен быть размещен внутри или в непосредственной близости от самого дальнего на шлейфе датчика. Данная мера необходима для четкого и своевременного обнаружения обрывов шлейфа или его короткого замыкания!



Приложение С. Процедура работы двух (основной и резервной) SIM-карт.

1. Проверка в профиле устройства активности основной SIM-карты. Если карта установлена как активная, то продолжить, если нет, то перейти на п. 3
2. Проверка нахождения в первом отсеке основной SIM-карты. Если SIM-карта присутствует и работоспособна, то продолжать работу до возникновения Условий Перехода На Резервную Карту. Иначе продолжить.
3. Проверка в профиле устройства активности основной SIM-карты. Если карта установлена как активная, то продолжить, если нет, то перейти на п. 1
4. Проверка нахождения во втором отсеке резервной SIM-карты. Если SIM-карта присутствует и работоспособна, то продолжить алгоритм. Иначе, в памяти терминала фиксируется отсутствие SIM-карты и обращений к ней до полной перезагрузки терминала происходить не будет. Терминал перейдет обратно на использование основной SIM-карты.
5. Активируется резервная карта и запускается таймер переключения (время таймера настраивается в утилите конфигурации) на основную карту.
6. По окончании времени таймера терминал переходит на использование основной SIM-карты (п.1).

Условия перехода на резервные SIM-карты:

- некоторое количество (варьируются в зависимости от версии прошивки микроконтроллера терминала) неудачных попыток подключения к серверу.
- некоторое количество (варьируются в зависимости от версии прошивки микроконтроллера терминала) неудачных попыток отправки SMS-сообщений.



Приложение D. Извещения от встроенных индикаторов.

Таблица 10

№	Цвет индикатора	Вид сигнала	Значение сигнала
1	Зеленый	постоянное свечение	электропитание подключено
2	Оранжевый	мигание с частотой 3-5 Гц	поиск GSM сети
3	Оранжевый	мигание 0,3-0,2 Гц	уверенный прием GSM сети
4	Синий	выключен	снят с охраны
5	Синий	мигание с частотой 2 Гц	постановка на охрану (самотестирование)
6	Синий Красный	мигание с частотой 0,5 Гц выключен	режим «Норма» взят под охрану
7	Синий Красный	мигание с частотой 0,5 Гц мигание с частотой 1 Гц	режим «Тревога», нарушен один из ШСБ
8	Синий	мигание с частотой 5 Гц	режим занесения в базу идентификационных признаков идентификатора электронного мастер-ключа
9	Синий Красный	мигание с частотой 5 Гц мигание с частотой 5 Гц	режим занесения/удаления в базу идентификационных признаков идентификаторов электронного ключа пользователей
10	Синий	постоянное свечение течение 2-х секунд	в идентификатор электронного ключа пользователя добавлен в базу идентификационных признаков электронных ключей пользователей
11	Красный	постоянное свечение течение 2-х секунд	в идентификатор электронного ключа пользователя удален из базы идентификационных признаков электронных ключей пользователей