



Бастион-2 – Elsys. Руководство  
администратора

Версия 1.2.11

(14.11.2020)



Самара, 2020

## Оглавление

<b>1</b>	<b>ОБЩИЕ СВЕДЕНИЯ</b> .....	<b>5</b>
<b>2</b>	<b>ЛИЦЕНЗИРОВАНИЕ</b> .....	<b>8</b>
<b>3</b>	<b>ДОБАВЛЕНИЕ ДРАЙВЕРА «БАСТИОН-2 – ELSYS»</b> .....	<b>8</b>
3.1	ДОБАВЛЕНИЕ ДРАЙВЕРА .....	8
3.2	ФУНКЦИИ ДРАЙВЕРА .....	8
<b>4</b>	<b>ПОИСК КОНТРОЛЛЕРОВ</b> .....	<b>9</b>
4.1	ПОИСК СЕТЕВЫХ КОНТРОЛЛЕРОВ .....	11
4.2	ПОИСК КОНТРОЛЛЕРОВ ДОСТУПА ELSYS-MB .....	13
4.3	ПОИСК КОНТРОЛЛЕРОВ ДОСТУПА ELSYS-MB-IP .....	17
<b>5</b>	<b>КОНФИГУРАТОР ОБОРУДОВАНИЯ</b> .....	<b>21</b>
5.1	СВОЙСТВА ДРАЙВЕРА «БАСТИОН-2 – ELSYS» .....	24
5.1.1	Вкладка «Основные» .....	24
5.1.2	Вкладка «Дополнительные».....	26
5.2	НАСТРОЙКА СЕТЕВЫХ КОНТРОЛЛЕРОВ ELSYS-MB-NET .....	27
5.2.1	Вкладка «Основные» .....	29
5.2.1.1	Настройки для линии связи RS-485 сетевого контроллера .....	31
5.2.1.2	Настройки для локальной сети.....	32
5.2.2	Вкладка «Дополнительные».....	32
5.2.2.1	Дополнительные настройки для локальной сети .....	32
5.2.2.2	Дополнительные настройки для линии связи RS-485 .....	33
5.3	НАСТРОЙКА СЕТЕВЫХ ГРУПП КОНТРОЛЛЕРОВ ELSYS-MB-IP .....	34
5.3.1	Режим передачи данных.....	35
5.3.2	Протокол обмена.....	36
5.3.3	Глобальный контроль последовательности прохода .....	37
5.3.4	Настройка обмена данными между контроллерами в сетевой группе .....	37
5.4	НАСТРОЙКА ЛИНИЙ СВЯЗИ RS-485, ПОДКЛЮЧЕННЫХ К COM-ПОРТУ .....	37
5.4.1	Вкладка «Основные» .....	38
5.4.2	Вкладка «Дополнительные».....	39
5.4.3	Настройка параметров преобразователя интерфейса Elsys-CU-USB/232-485.....	39
5.5	НАСТРОЙКА КОНТРОЛЛЕРОВ ELSYS-MB .....	40
5.5.1	Вкладка «Основные» .....	42
5.5.2	Вкладка «Дополнительные».....	46
5.5.3	Вкладка «Контроль последовательности прохода» .....	47
5.6	НАСТРОЙКА КОНТРОЛЛЕРОВ ELSYS-MB-IP .....	49
5.7	РАБОТА С КОНФИГУРАЦИЯМИ КОНТРОЛЛЕРОВ ELSYS-MB И ELSYS-MB-IP .....	51
5.7.1	Использование готовых конфигураций.....	51
5.7.2	Копирование и вставка конфигурации .....	61
5.7.3	Сохранение и загрузка конфигурации .....	64
5.8	НАСТРОЙКА ТОЧЕК ДОСТУПА .....	66
5.8.1	Добавление точек доступа и считывателей.....	66
5.8.2	Настройка двери с односторонним контролем доступа .....	68
5.8.3	Настройка двери с двусторонним контролем доступа .....	70
5.8.4	Настройка турникета.....	71
5.8.5	Настройка ворот и шлагбаумов .....	72
5.9	НАСТРОЙКА ВХОДОВ .....	74
5.9.1	Описание настроек входов .....	74
5.9.2	Использование входов.....	79
5.9.3	Особенности настройки входов в зависимости от их функционального назначения .....	82

5.10	НАСТРОЙКА ОХРАННЫХ ФУНКЦИЙ .....	83
5.10.1	Структура охранной подсистемы .....	83
5.10.2	Настройка охранных функций без использования разделов .....	84
5.10.3	Настройка охранных функций с использованием разделов .....	84
5.10.4	Настройка световой и звуковой индикации состояний разделов .....	89
5.10.5	Настройка исполнительных устройств охранной подсистемы .....	89
5.11	НАСТРОЙКА ВЫХОДОВ И ГРУПП ВЫХОДОВ .....	92
5.11.1	Настройка выходов .....	92
5.11.2	Настройка групп выходов .....	93
5.12	НАСТРОЙКА СЧИТЫВАТЕЛЕЙ .....	95
5.12.1	Вкладка «Основные» .....	95
5.12.2	Вкладка «Дополнительные» .....	99
5.12.3	Вкладка «Доступ по нескольким картам» .....	101
5.12.4	Вкладка «Биометрический считыватель» .....	102
5.13	ОСОБЕННОСТИ НАСТРОЙКИ КОНТРОЛЛЕРОВ ELSYS-MB-SM .....	105
5.13.1	Настройка контроллеров .....	106
5.13.2	Настройка дверей .....	106
5.13.3	Настройка считывателей .....	107
5.14	ОСОБЕННОСТИ НАСТРОЙКИ МОДУЛЕЙ ELSYS-IO/MB .....	107
5.15	ОСОБЕННОСТИ НАСТРОЙКИ ОХРАННЫХ КОНТРОЛЛЕРОВ ELSYS-MB-AC .....	108
5.15.1	Настройки контроллеров .....	108
5.15.2	Настройка входов .....	108
5.15.3	Настройка выходов .....	109
5.15.4	Настройка охранных разделов .....	109
5.15.5	Настройка исполнительных устройств охранной подсистемы .....	111
5.15.6	Группы управления охраной .....	111
5.15.7	Настройка взаимодействий .....	112
5.16	УПРАВЛЕНИЕ УСТРОЙСТВАМИ ИЗ КОНФИГУРАТОРА ОБОРУДОВАНИЯ .....	113
5.17	УСТАНОВКА ОГРАНИЧЕНИЙ ДОСТУПА К РАЗЛИЧНЫМ ФУНКЦИЯМ ДРАЙВЕРА .....	115
<b>6</b>	<b>НАСТРОЙКА ГЛОБАЛЬНОГО КОНТРОЛЯ ПОСЛЕДОВАТЕЛЬНОСТИ ПРОХОДА .....</b>	<b>117</b>
6.1	ОПИСАНИЕ РАБОТЫ ГЛОБАЛЬНОГО КОНТРОЛЯ ПОСЛЕДОВАТЕЛЬНОСТИ ПРОХОДА .....	117
6.2	НАСТРОЙКА ОБОРУДОВАНИЯ ДЛЯ РАБОТЫ ГЛОБАЛЬНОГО КОНТРОЛЯ ПОСЛЕДОВАТЕЛЬНОСТИ ПРОХОДА .....	120
6.2.1	Настройка в одной линии связи .....	121
6.2.2	Настройка в линиях связи сетевых контроллеров .....	122
6.3	НАСТРОЙКА ОБЛАСТЕЙ КОНТРОЛЯ .....	123
6.4	ДИАГНОСТИКА ГЛОБАЛЬНОГО КОНТРОЛЯ ПОСЛЕДОВАТЕЛЬНОСТИ ПРОХОДА .....	124
6.5	ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ ГЛОБАЛЬНОГО КОНТРОЛЯ ПОСЛЕДОВАТЕЛЬНОСТИ ПРОХОДА .....	128
6.5.1	Мягкий antipassback .....	128
6.5.2	Настройка «Сброс в полночь» .....	129
6.5.3	Временной antipassback .....	129
6.5.4	Настройка «Не проверять исправность областей контроля» .....	129
6.5.5	Настройка «Усиленный antipassback» .....	130
6.5.6	Индивидуальная настройка «не отслеживать последовательность прохода» .....	130
6.6	ПРИМЕР НАСТРОЙКИ ГЛОБАЛЬНОГО КОНТРОЛЯ ПОСЛЕДОВАТЕЛЬНОСТИ ПРОХОДА .....	131
<b>7</b>	<b>ИНИЦИАЛИЗАЦИЯ И УПРАВЛЕНИЕ КОНТРОЛЛЕРАМИ .....</b>	<b>135</b>
7.1	ИНИЦИАЛИЗАЦИЯ КОНТРОЛЛЕРОВ .....	135
7.2	УПРАВЛЕНИЕ КОНТРОЛЛЕРАМИ .....	141
7.3	ВОССТАНОВЛЕНИЕ ПРОТОКОЛА СОБЫТИЙ .....	143
<b>8</b>	<b>ПРОВЕРКА ТЕКУЩЕГО СОСТОЯНИЯ КОНТРОЛЛЕРОВ .....</b>	<b>145</b>
8.1	ПРОВЕРКА КОНФИГУРАЦИИ КОНТРОЛЛЕРОВ .....	145

8.2	ПРОВЕРКА НАЛИЧИЯ СВЯЗИ С КОНТРОЛЛЕРАМИ .....	147
<b>9</b>	<b>ДОПОЛНИТЕЛЬНЫЕ СВЕДЕНИЯ ПО НАСТРОЙКЕ ДРАЙВЕРА «БАСТИОН-2 – ELSYS» .....</b>	<b>148</b>
9.1	СИСТЕМА ПРОГРАММИРУЕМЫХ АППАРАТНЫХ ВЗАИМОДЕЙСТВИЙ.....	148
9.1.1	<i>Настройка взаимодействий.....</i>	149
9.1.2	<i>Настройка формул управления работой выходов .....</i>	151
9.1.3	<i>Логические формулы.....</i>	152
9.1.4	<i>Счётчики событий.....</i>	154
9.1.5	<i>Взаимодействия между контроллерами .....</i>	155
9.1.6	<i>Служебные PIN-коды .....</i>	158
9.1.7	<i>Назначение реакций на предъявление отдельных карт доступа .....</i>	160
9.1.8	<i>Назначение реакций на удержание ключа/карты .....</i>	161
9.1.9	<i>Настройка управления по временным расписаниям .....</i>	163
9.1.9.1	<i>Настройка временных расписаний .....</i>	163
9.1.9.2	<i>Настройка взаимодействий по временным расписаниям .....</i>	165
9.1.9.3	<i>Настройка логических формул с использованием временных расписаний.....</i>	166
9.1.10	<i>Настройка функций, связанных с подсчётом персонала .....</i>	167
9.2	ПРОФИЛИ НАСТРОЕК ПЕРСОНАЛА .....	169
9.3	НАСТРОЙКА АВТОМАТИЧЕСКОЙ ПОСТАНОВКИ РАЗДЕЛА НА ОХРАНУ ПРИ ВЫХОДЕ ПОСЛЕДНЕГО СОТРУДНИКА .....	176
9.4	СОБЫТИЯ ДРАЙВЕРА «БАСТИОН-2 – ELSYS» .....	179
9.4.1	<i>События выходов и групп выходов .....</i>	179
9.4.2	<i>События точек доступа.....</i>	180
9.4.3	<i>События входов .....</i>	185
9.4.4	<i>События контроллеров .....</i>	187
9.4.5	<i>События разделов .....</i>	190
9.4.6	<i>События сетевых контроллеров Elsys-MB-Net.....</i>	190
9.4.7	<i>События, формируемые драйвером «Бастсион-2 – Elsys» .....</i>	191
9.4.8	<i>События биометрических считывателей.....</i>	192
	КОМАНДЫ КОНТРОЛЛЕРОВ ELSYS-MB .....	192
9.5	ИНДИКАЦИЯ СОСТОЯНИЯ УСТРОЙСТВ И РАЗДЕЛОВ НА ПЛАНАХ .....	194
9.6	ПОРТЫ ПРОТОКОЛОВ TCP/IP и UDP/IP, ИСПОЛЬЗУЕМЫЕ КСК ELSYS-MB-NET И КОНТРОЛЛЕРАМИ ELSYS-MB-IP ...	201
<b>10</b>	<b>ОКНО «БИОМЕТРИЯ».....</b>	<b>205</b>
<b>11</b>	<b>ПОРЯДОК НАСТРОЙКИ СКУД ELSYS ДЛЯ РАЗЛИЧНЫХ РЕЖИМОВ РАБОТЫ.....</b>	<b>208</b>
11.1	ОБЩИЕ НАСТРОЙКИ ПО «БАСТИОН-2», ИСПОЛЬЗУЕМЫЕ В РАБОТЕ ДРАЙВЕРА «БАСТИОН-2 – ELSYS» .....	208
11.2	НАСТРОЙКА СИСТЕМЫ ПРИ ИСПОЛЬЗОВАНИИ ДВОЙНОЙ ИДЕНТИФИКАЦИИ (PIN-КОД И КАРТА).....	208
11.3	ДОСТУП С ПОДТВЕРЖДЕНИЕМ КАРТОЙ .....	209
11.4	ДОСТУП С ПОДТВЕРЖДЕНИЕМ ОПЕРАТОРОМ.....	213
11.5	ДОСТУП С ИСПОЛЬЗОВАНИЕМ БИОМЕТРИЧЕСКИХ СЧИТЫВАТЕЛЕЙ.....	214
	<b>ПРИЛОЖЕНИЯ .....</b>	<b>216</b>
	ПРИЛОЖЕНИЕ 1. ИСТОРИЯ ИЗМЕНЕНИЙ.....	216

## 1 Общие сведения

Драйвер «Бастион-2 – Elsys» предназначен для настройки параметров, мониторинга и управления системы контроля и управления доступом (СКУД) Elsys (ООО НИЦ «ФОРС», Ассоциация «Электронные системы»).

Драйвер обеспечивает поддержку всей номенклатуры оборудования СКУД Elsys - контроллеров доступа Elsys-MB вариантов исполнения Pro, Standard, Light, Pro4, SM, модулей Elsys-IO/MB, коммуникационных сетевых контроллеров Elsys-MB-Net (далее – КСК).

Кроме того, драйвер позволяет в своём составе использовать биометрические контроллеры торговых марок ЛКД, Elsys, Suprema и EnterFace в качестве биометрических считывателей. При этом биометрические контроллеры должны быть подключены к контроллерам доступа СКУД Elsys по интерфейсу Wiegand, а также в локальную сеть Ethernet. Драйвер поддерживает следующие типы биометрических контроллеров: ЛКД КО-60 00, ЛКД КО-15 00, ЛКД КО-75 00, Elsys-PVR, EnterFace 3D, EnterFace 3D Gate, Suprema. В качестве биометрических признаков могут использоваться следующие типы сигнатур: отпечатки пальцев (ЛКД КО-60 00, ЛКД КО-15 00, ЛКД КО-75 00, Suprema), рисунок вен ладони (Elsys-PVR) и геометрия лица (EnterFace 3D, EnterFace 3D Gate).

Обобщённая структурная схема СКУД Elsys приведена на рисунке 1.

Контроллеры Elsys-MB вариантов исполнения Pro, Standard, Light, Pro4, SM, модули Elsys-IO/MB могут быть объединены в сеть по двухпроводному интерфейсу RS-485 (до 63 контроллеров в одной линии связи) и подключены к компьютеру одним из двух способов:

- через преобразователь интерфейсов Elsys-RC-232/485 или Elsys-CU-USB-232/485 соответственно к COM или USB порту персонального компьютера;
- через коммуникационный сетевой контроллер Elsys-MB-Net (далее – КСК), обеспечивающий обмен данными с ПК через локальную вычислительную сеть Ethernet.

Кроме того, контроллеры Elsys-MB старших моделей (Pro, Standard, Light, Pro4) могут быть оснащены интерфейсным Ethernet-модулем Elsys-IP (в этом случае они обозначаются как Elsys-MB-IP) и подключены к ПК через локальную вычислительную сеть Ethernet.

Контроллеры Elsys-MB-IP в количестве до 63 могут быть объединены в сетевые группы (СГ), в пределах каждой из которых возможен обмен информацией контроллеров между собой. Для обеспечения обмена данными с контроллерами из других линий связи или сетевых групп в сетевую группу может входить также КСК Elsys-MB-Net.

КСК Elsys-MB-Net, предназначенные для интеграции контроллеров Elsys-MB и Elsys-MB-IP в единую систему, включаются в локальную вычислительную сеть Ethernet.

Каждый экземпляр драйвера «Бастион-2 – Elsys» работает с назначенными COM-портами, а также поддерживает до 255 КСК и до 254 сетевых групп.

**Внимание!** Перед началом настройки СКУД Elsys необходимо ознакомиться с документами «Руководство системного администратора», «Рекомендации по комплектации и проектированию СКУД Elsys», «Руководство по эксплуатации СКУД



*Elsys», а также с руководствами по эксплуатации на всё используемое оборудование.*

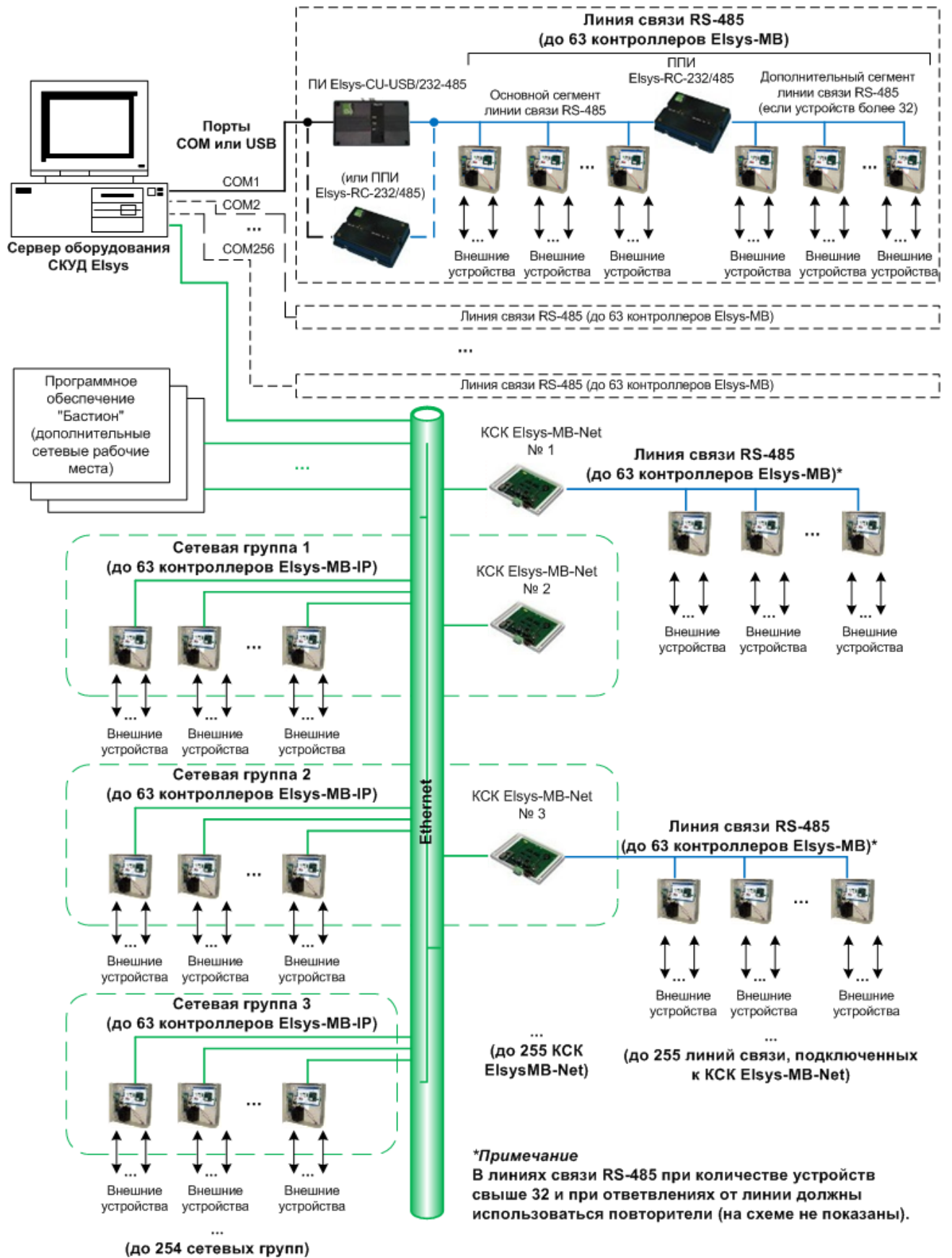


Рисунок 1 - Структурная схема СКУД Elsys

## 2 Лицензирование

Правила комплектации и лицензирования модуля (драйвера) рассмотрены в документе «Пособие по комплектации «Бастион-2».

## 3 Добавление драйвера «Бастион-2 – Elsys»

**Внимание!** Перед началом работы с драйвером «Бастион-2 – Elsys» необходимо ознакомиться с «Руководством системного администратора».

### 3.1 Добавление драйвера

Добавление драйвера в Бастион версии 2.0.5 и выше описано в документе «Бастион-2. Руководство администратора», который находится в папке «Bastion2\Docs».

### 3.2 Функции драйвера

После добавления драйвера и перезапуска ПО «Бастион-2» на вкладке **«Драйверы»** появится лента управления драйвером **«Драйвер СКУД «Elsys»** (рисунок 2).

Кнопка **«Конфигурация оборудования»** вызывает конфигуратор оборудования, предназначенный для изменения структуры системы и настройки параметров контроллеров.

Кнопка **«Профили настроек персонала»** позволяет настроить дополнительные полномочия пользователя, обеспечивающие организацию специфических условий доступа (более подробно см. п. 9.2).

Кнопка **«Проверка конфигурации»** позволяет проверить состояние контроллеров (в частности, число карт, уровней доступа и т. д.), а также проверить наличие связи с ними (более подробно см. п. 8).

Кнопка **«Поиск устройств»** позволяет выполнить поиск, настройку параметров и добавление в базу данных заранее подключенных сетевых контроллеров Elsys-MB-Net и контроллеров доступа Elsys-MB (более подробно см. п. 4).

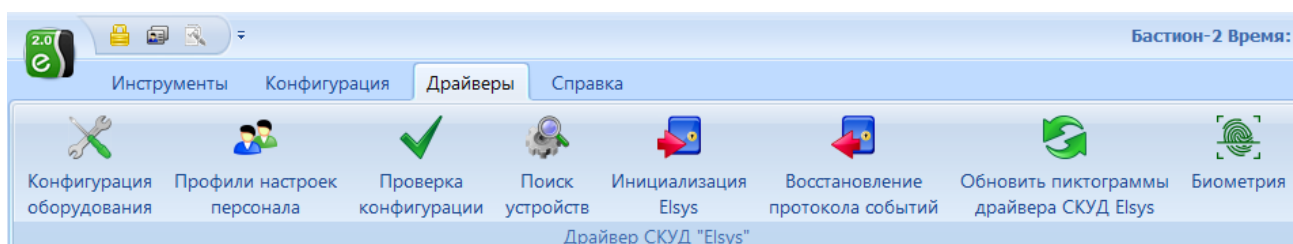


Рисунок 2 - Лента управления драйвером «Бастион-2 – Elsys»

Кнопка **«Инициализация Elsys»** позволяет записать настройки оборудования, карты доступа и уровни доступа в сетевые контроллеры, и контроллеры доступа Elsys-MB. (более подробно см. п. 7).



Кнопка **«Восстановление протокола событий»** позволяет прочитать события из контроллеров за указанный интервал времени, если произошёл сбой с потерей данных (более подробно см. п. 6).

При нажатии на кнопку **«Обновить пиктограммы драйвера СКУД Elsys»** всем контроллерам СКУД «Elsys» отправляется запрос состояний устройств, в результате иконки соответствующих устройств на планах перекрашиваются.

Кнопка **«Биометрия»** открывает окно для работы с биометрическими считывателями. Этот режим позволяет проверить состояние биометрических считывателей, выполнить их инициализацию (записать карты и сигнатуры), а также выполнять команды сброса и очистки конфигурации (более подробно см. п. 10).

Если какие-то кнопки ленты управления драйвером СКУД «Elsys» недоступны, значит, в настройках профиля оператора отсутствуют соответствующие разрешения.

***Внимание!** В драйвере «Бастيون-2 – Elsys» режимы редактирования конфигурации, инициализации оборудования и поиска контроллеров, которые выполняются на разных рабочих местах, являются взаимоисключающими.*

## 4 Поиск контроллеров

Функция поиска предназначена для обнаружения подключенных контроллеров Elsys-MB, Elsys-MB-IP и Elsys-MB-Net, первоначальной настройки и занесения информации в базу данных.

***Внимание!** В ПО «Бастيون-2» в один экземпляр драйвера СКУД «Elsys» можно добавить не более 255 КСК и не более 254 СГ.*

Окно поиска контроллеров вызывается с помощью кнопки **«Поиск устройств...»** на ленте управления драйвером (см. рисунок 2).

***Внимание!** Поиск не работает во время запуска драйвера и первоначального опроса контроллеров. Во время обработки изменений конфигурации поиск может выполняться с задержками.*

Окно поиска контроллеров (рисунок 3) имеет три вкладки — **«Поиск сетевых контроллеров»** для поиска сетевых контроллеров, **«Поиск контроллеров Elsys-MB»** для поиска контроллеров доступа Elsys-MB, **«Поиск контроллеров Elsys-MB-IP»** для поиска контроллеров доступа Elsys-MB-IP.

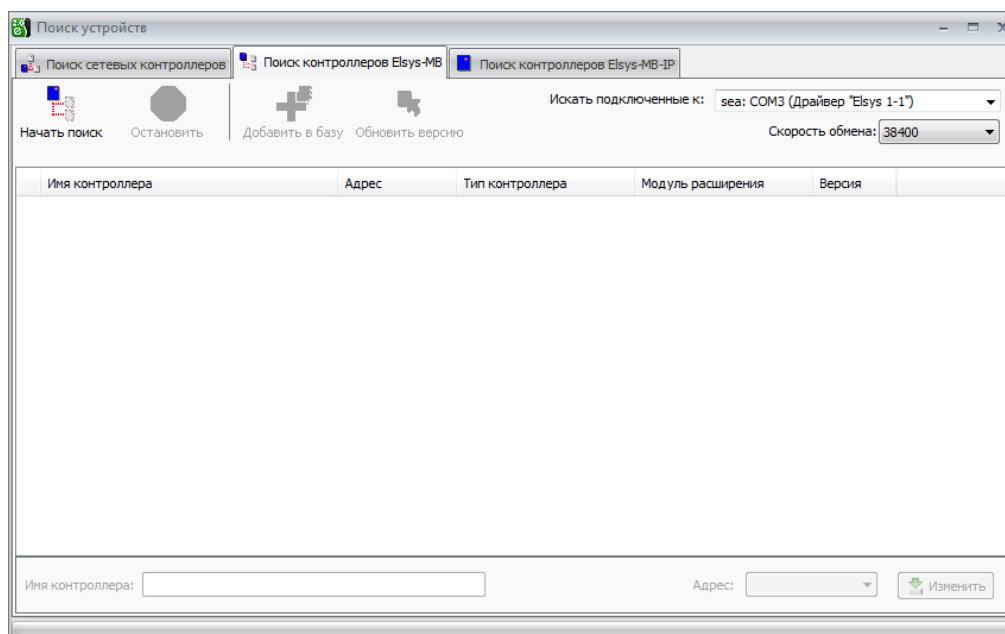


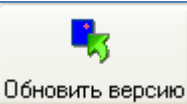


Рисунок 3- Окно поиска контроллеров

Назначение кнопок на панели управления в окне поиска контроллеров приведено в таблице 1.

Таблица 1– Назначение кнопок на панели управления в окне поиска контроллеров

Кнопка	Наименование	Кнопка быстрого доступа	Назначение
	«Начать поиск»	F3	Запускает поиск сетевых контроллеров.  Доступна только на вкладке «Поиск сетевых контроллеров».
	«Начать поиск»	F3	Запускает поиск контроллеров доступа Elsys-MB.  Доступна только на вкладке «Поиск контроллеров Elsys-MB».
	«Начать поиск»	F3	Запускает поиск контроллеров доступа Elsys-MB IP.  Доступна только на вкладке «Поиск контроллеров Elsys-MB-IP».

 Остановить	<b>«Остановить»</b>	Esc	Останавливает поиск сетевых контроллеров или контроллеров доступа.
 Добавить в базу	<b>«Добавить в базу»</b>	Ctrl+S	Добавляет в базу данных выбранный контроллер.
 Обновить версию	<b>«Обновить версию»</b>		Обновляет номер версии ПО контроллера в базе данных, если она отличается от версии найденного прибора.




#### 4.1 Поиск сетевых контроллеров

Перед поиском сетевых контроллеров необходимо подключить их к компьютерной сети, подать питание и проверить соединение с сетью по индикаторам на сетевом контроллере и на Ethernet-концентраторах.

Для поиска сетевых контроллеров необходимо выбрать вкладку **«Поиск сетевых контроллеров»** в окне поиска контроллеров (рисунок 4) и нажать кнопку **«Начать поиск»**.

Если необходимо прервать процесс поиска, нужно нажать кнопку **«Остановить»**.

Найденные сетевые контроллеры отображаются следующими пиктограммами:

-  - Сетевой контроллер, с таким же IP адресом и номером отсутствует в базе данных (новый сетевой контроллер).
-  - Сетевой контроллер, с таким же IP адресом и номером уже добавлен в базу (существующий сетевой контроллер). К наименованию данного контроллера добавляется надпись «(есть в базе)».
-  - Сетевой контроллер, с таким же IP адресом и номером уже добавлен в базу, но имеет более старую версию.

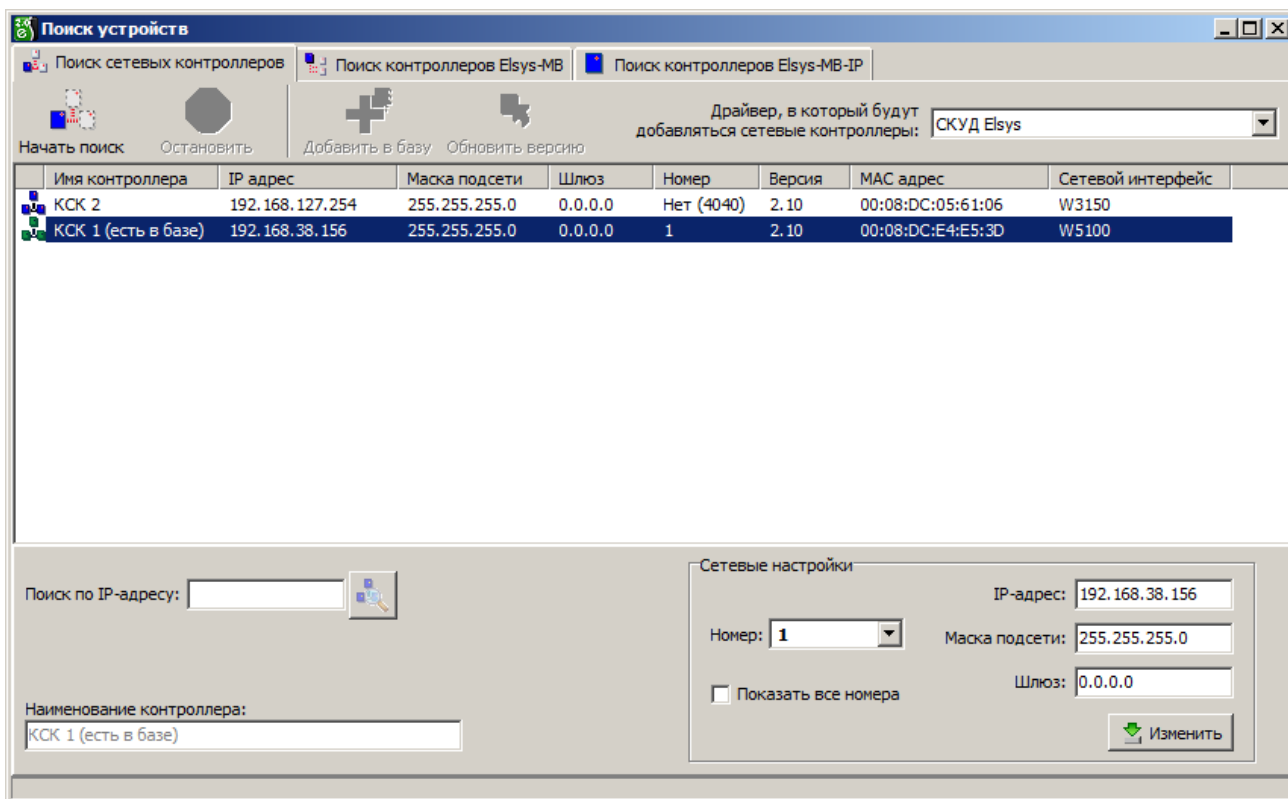
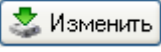



Рисунок 4 - Окно с результатами поиска сетевых контроллеров

Контроллеры с настройками по умолчанию имеют IP-адрес 192.168.127.254 и номер 4040h. Настроить параметры сетевого контроллера можно непосредственно из окна поиска. Для этого необходимо выделить сетевой контроллер и указать нужные значения IP-адреса, маски подсети, IP-адреса шлюза и номера контроллера в группе параметров **«Сетевые настройки»** внизу окна поиска и нажать кнопку , после чего новые настройки будут записаны в сетевой контроллер.

Настройка **«Показать все номера»** необходима, если сетевому контроллеру требуется присвоить номер, уже существующий в базе. Если эта настройка включена, номера, присутствующие в базе, в выпадающем списке **«Номер»** будут отображаться цифрой на красном фоне.

Для сетевых контроллеров с установленными сетевыми настройками существует возможность поиска по IP-адресу, для этого необходимо ввести IP-адрес искомого сетевого контроллера в поле **«Поиск по IP-адресу»** и нажать кнопку  (рисунок 5).

**«Наименование контроллера»** – наименование контроллера, которое можно изменить в целях более удобного представления информации.

После того как все настройки сделаны, сетевой контроллер может быть добавлен в базу данных кнопкой **«Добавить в базу»**.

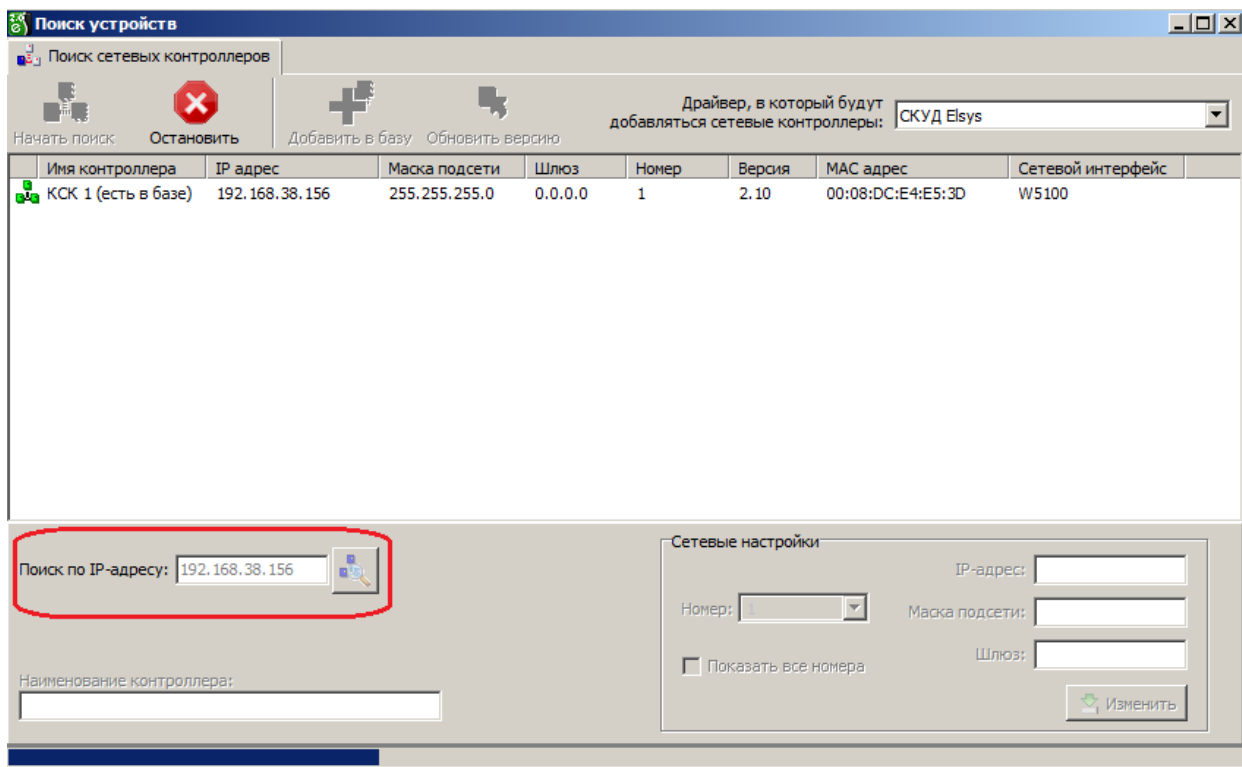


Рисунок 5 - Поиск сетевого контроллера по IP-адресу

Выпадающее меню **«Драйвер, в который будут добавляться сетевые контроллеры»** предназначено для выбора экземпляра драйвера (если в системе добавлено более одного драйвера «Бастион-2 – Elsys»), в который будет добавляться сетевой контроллер.

Если в списке есть один или несколько сетевых контроллеров, для которых необходимо обновить версию, достаточно нажать кнопку **«Обновить версию»** и информация о версии для всех контроллеров будет записана в базу.

Если сетевой контроллер не находится поиском, возможны следующие причины:

- неисправность линии связи до сетевого контроллера;
- несоответствие паролей. Если в контроллер уже были записаны один раз настройки, то автоматически туда был записан и пароль (рисунок 16), если пароли в настройках драйвера и в сетевом контроллере не совпадают, то он находится не будет. В этом случае необходимо произвести аппаратную очистку конфигурации сетевого контроллера в соответствии с руководством по эксплуатации.

Если не активна кнопка «Добавить в базу», значит IP-адрес или номер выделенного контроллера уже есть в базе данных, либо сетевой контроллер имеет настройки по умолчанию.

## 4.2 Поиск контроллеров доступа Elsys-MB

Если контроллеры доступа подключены к сетевым контроллерам, то необходимо сначала выполнить начальную настройку КСК (назначить им номер, IP-адрес, маску подсети и адрес

шлюза), добавить их в базу, дождаться установления с ними связи, после чего приступить к поиску контроллеров Elsys-MB.

Перед началом поиска следует убедиться, что скорость обмена в настройках драйвера (или сетевого контроллера, если линия связи подключена к нему), в преобразователе интерфейсов (если линия связи подключена к COM-порту) и в контроллерах доступа, относящихся к выбранной линии связи, установлена одинаковой. Установка скорости обмена описана в руководствах по эксплуатации на соответствующее оборудование.

В контроллерах Elsys-MB старших вариантов исполнения и в контроллерах Elsys-MB-SM скорость обмена устанавливается DIP-переключателями SW1.7 – SW1.9, в соответствии с руководством по эксплуатации.

В контроллерах более ранних версий, не имевших DIP-переключателей, скорость выставляется кнопкой CLEAR (необходимо длительно удерживать эту кнопку, и через каждые 5 секунд будет устанавливаться новое значение скорости; частота мигания индикатора RUN 5 Гц соответствует скорости 38400 бит/с).

В преобразователе интерфейсов Elsys-CU-USB/232-485 скорость обмена выбирается автоматически. В преобразователе Elsys-RC-232/485 скорость обмена устанавливается переключками.

Перед началом работы каждому контроллеру должен быть присвоен уникальный, в пределах каждой линии связи адрес. Адреса контроллерам следует задавать, начиная с № 1, в порядке возрастания, без пропусков.

Если линий связи несколько, в каждой линии следует задавать нумерацию заново, начиная с 1.

Если эти требования не будут выполнены, эффективность обмена данными с контроллерами может значительно снизиться. Так, при произвольной адресации в линии связи, время инициализации оборудования может возрасти в несколько раз.

Поиск контроллеров осуществляется отдельно для каждой линии связи RS-485, подключенной к COM-портам или контроллерам Elsys-MB-Net. Выбор линии связи, в которой будет выполняться поиск, осуществляется в выпадающем меню **«Искать подключенные к ...»** (рисунок 6).

Перед выполнением поиска в выбранной линии связи должен быть выбран режим обмена MASTER-SLAVE. Если был включен режим MULTIMASTER, будет предложено его выключить и затем начать поиск, либо отказаться от поиска.

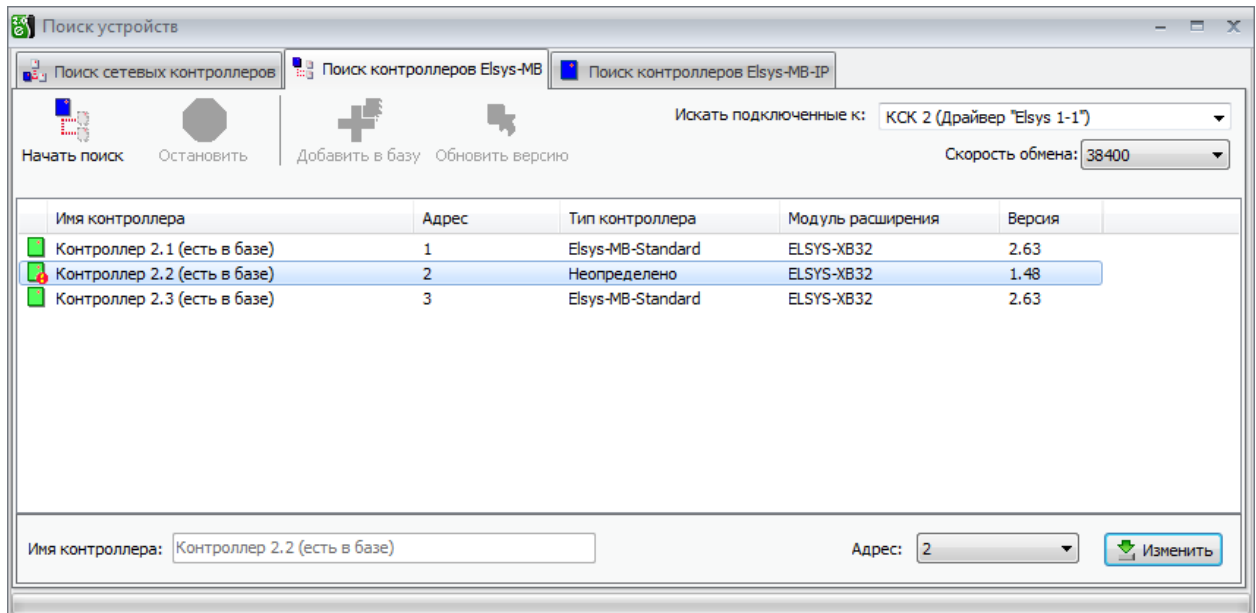






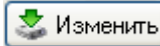
Рисунок 6- Окно с результатами поиска контроллеров доступа Elsys-MB

Для поиска контроллеров необходимо выбрать вкладку **«Поиск контроллеров»** в окне поиска контроллеров (рисунок 6) и нажать кнопку **«Начать поиск»**.

Если необходимо прервать процесс поиска, нужно нажать кнопку **«Остановить»**.

Найденные контроллеры отображаются следующими пиктограммами:

-  - Контроллер с таким же адресом отсутствует в базе, либо это контроллер с настройками по умолчанию (новый контроллер).
-  - Контроллер, с таким же адресом уже добавлен в базу (существующий контроллер). К наименованию данного контроллера добавляется надпись «(есть в базе)».
-  - Контроллер, с таким же адресом уже добавлен в базу, но имеет более старую версию.
-  - Контроллер, найденный при поиске и контроллер, добавленный в базу, отличаются по типу контроллера или по типу (или наличию) модуля расширения.

Для контроллеров, не имеющих DIP-переключателей, задать новый адрес можно непосредственно из окна поиска. Для этого необходимо выделить контроллер, выбрать нужный адрес в выпадающем списке **«Адрес»** внизу окна поиска и нажать кнопку  **Изменить**, после чего новый адрес будет записан в контроллер.

**«Имя контроллера»** – наименование контроллера, которое можно изменить в целях более удобного представления информации.

После того, как все настройки сделаны, контроллер может быть добавлен в базу данных кнопкой **«Добавить в базу»**.

Для добавляемого контроллера будет предложено выбрать готовую конфигурацию, совместимую с его вариантом исполнения (рисунок 7), либо пустую конфигурацию.

После выбора готовой конфигурации контроллер будет добавлен в базу данных и автоматически проинициализирован (рисунок 8), после чего он полностью готов к работе.

Если при нажатии на кнопку **«Начать поиск»** ни одного прибора не было найдено, необходимо проверить следующее:

- правильность подключения к линии связи RS-485, при необходимости проконтролировав по светодиодным индикаторам прохождение сигналов (см. соответствующие руководства по эксплуатации);
- соответствие скоростей обмена в ПО «Бастион-2», в контроллерах и преобразователях интерфейсов;
- убедиться, что на линии связи нет контроллеров с одинаковыми адресами.

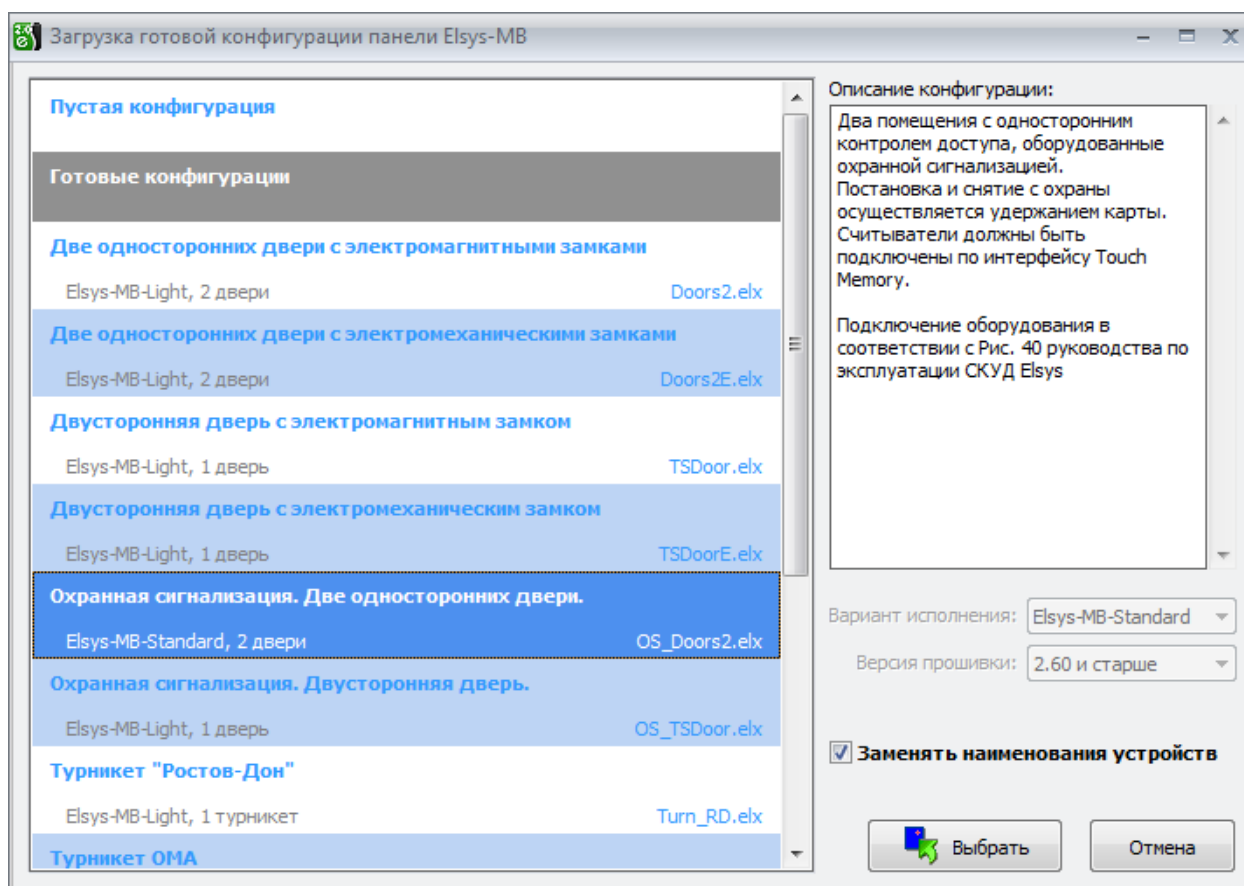


Рисунок 7 - Выбор готовой конфигурации контроллера при добавлении из поиска



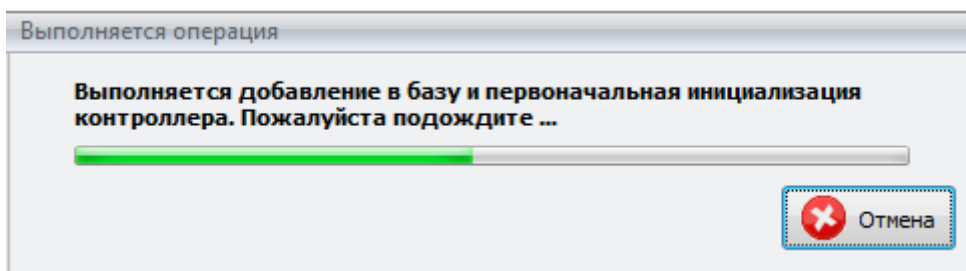


Рисунок 8 - Окно предупреждения об инициализации контроллера доступа

### 4.3 Поиск контроллеров доступа Elsys-MB-IP

Перед поиском контроллеров Elsys-MB-IP необходимо подключить их к компьютерной сети, подать питание и проверить соединение с сетью по индикаторам на интерфейсном Ethernet-модуле контроллера Elsys-MB-IP и на Ethernet-концентраторах.

Для поиска контроллеров Elsys-MB-IP необходимо выбрать вкладку «Поиск контроллеров Elsys-MB-IP» в окне поиска контроллеров (рисунок 9) и нажать кнопку «Начать поиск».

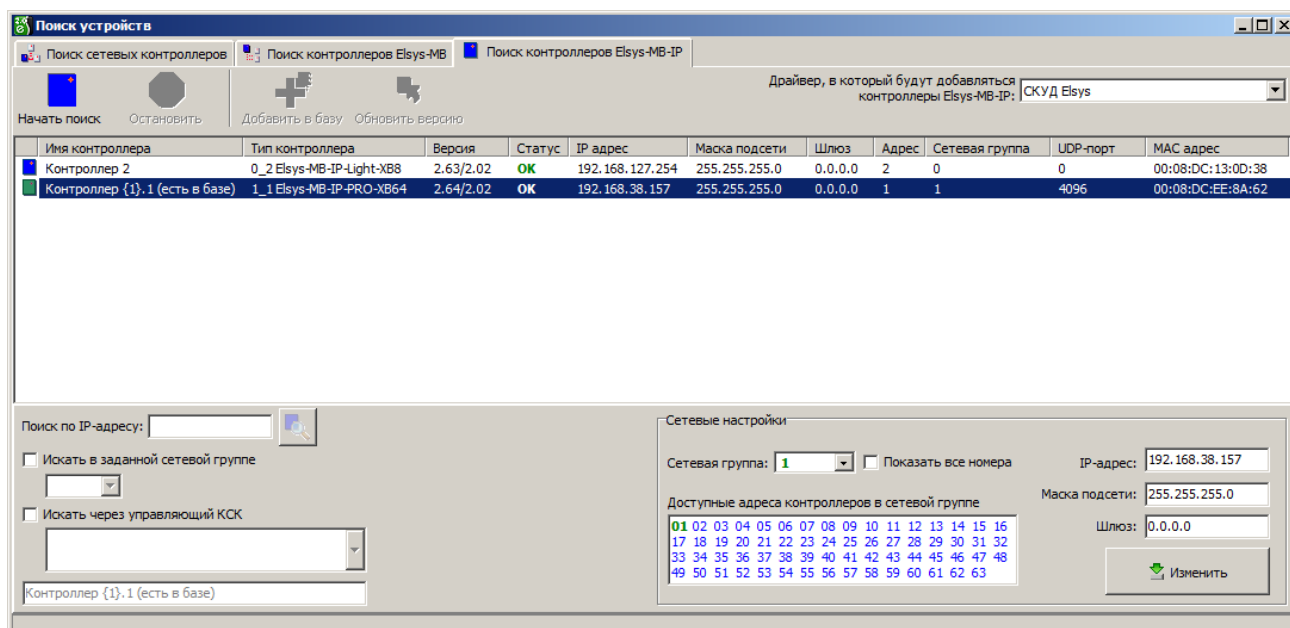
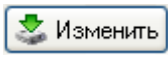


Рисунок 9 - Окно с результатами поиска контроллеров доступа Elsys-MB-IP

Если необходимо прервать процесс поиска, нужно нажать кнопку «Остановить».

Найденные контроллеры Elsys-MB-IP отображаются такими же пиктограммами, как и при поиске Elsys-MB (см. п. 4.2).

Контроллер Elsys-MB-IP с настройками по умолчанию имеет IP-адрес 192.168.127.254 и номер сетевой группы равный нулю.

Установить сетевые настройки контроллера Elsys-MB-IP можно непосредственно из окна поиска. Для этого необходимо выделить контроллер и задать требуемые значения номера сетевой группы, IP-адреса, маски подсети и IP-адреса шлюза в группе параметров «Сетевые настройки» и нажать кнопку , после чего новые настройки будут записаны в контроллер Elsys-MB-IP.

Номер сетевой группы лежит в диапазоне от 1 до 254 и выбирается из списка, который формируется с учетом существующих контроллеров Elsys-MB-IP и КСК. Номера существующих в БД СГ, в которых адрес текущего выбранного контролера не используется, отображаются зеленым цветом, номера СГ, которые отсутствуют в БД и могут быть добавлены в текущий драйвер – синим цветом, остальные номера отображаются черным цветом на красном фоне при включенной опции **«Показать все номера»**.

Опция **«Показать все номера»** используется, когда контроллеру требуется присвоить номер сетевой группы, а контроллер с таким номером группы и адресом уже есть в базе данных. Если эта настройка включена, номера существующих в БД сетевых групп, в которых есть контроллеры с таким же адресом будут отображаться на красном фоне (рисунок 10).

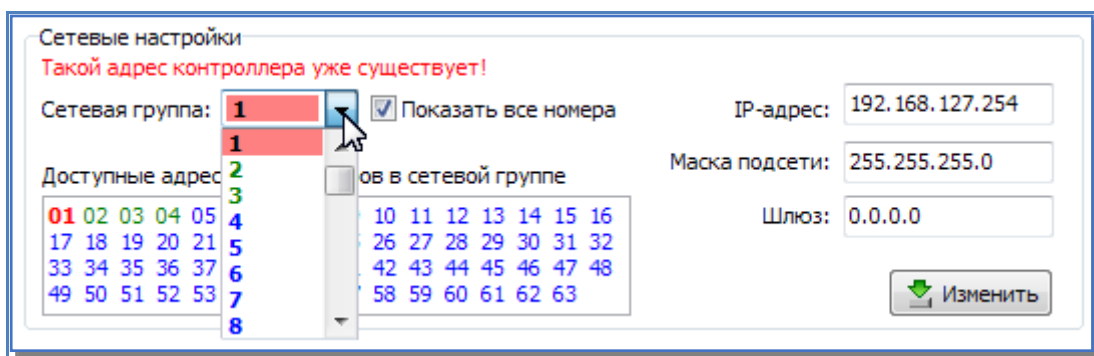


Рисунок 10 – Отображение номеров сетевых групп и доступных адресов контроллеров в сетевой группе

Таблица **«Доступные адреса контроллеров в сетевой группе»** предназначена для отображения свободных, занятых, а также конфликтующих адресов контроллеров (рисунок 10). Свободные (доступные) адреса отображаются синим цветом, занятые – зеленым, красным цветом отображаются занятые адреса, которые совпадают с адресом выбранного контроллера в результатах поиска.

Для контроллеров Elsys-MB-IP с установленными сетевыми настройками существует возможность поиска по IP-адресу, для этого необходимо ввести IP-адрес искомого

контроллера в поле **«Поиск по IP-адресу»** и нажать кнопку  (рисунок 11).

Настройка **«Искать в заданной сетевой группе»** позволяет указать номер сетевой группы, в пределах которой следует осуществлять поиск контроллеров Elsys-MB-IP (рисунок 12).

Если в конфигурации СКУД «Elsys» присутствуют сетевые группы, в которых установлен протокол обмена **«Через КСК по UDP»**, то доступна опция **«Искать через управляющий КСК»** (рисунок 13). Эта опция используется при поиске контроллеров Elsys-MB-IP и изменении их сетевых настроек, когда контроллеры Elsys-MB-IP находятся в подсетях, в которых не могут использоваться широковещательные UDP-пакеты. На рисунке 13 показан процесс поиска через управляющий КСК **«КСК 1»**, который управляет сетевой группой **«Сетевая группа {1}»**. На рисунке 14 показана кнопка изменения сетевых настроек контроллера Elsys-MB-IP через управляющий КСК.

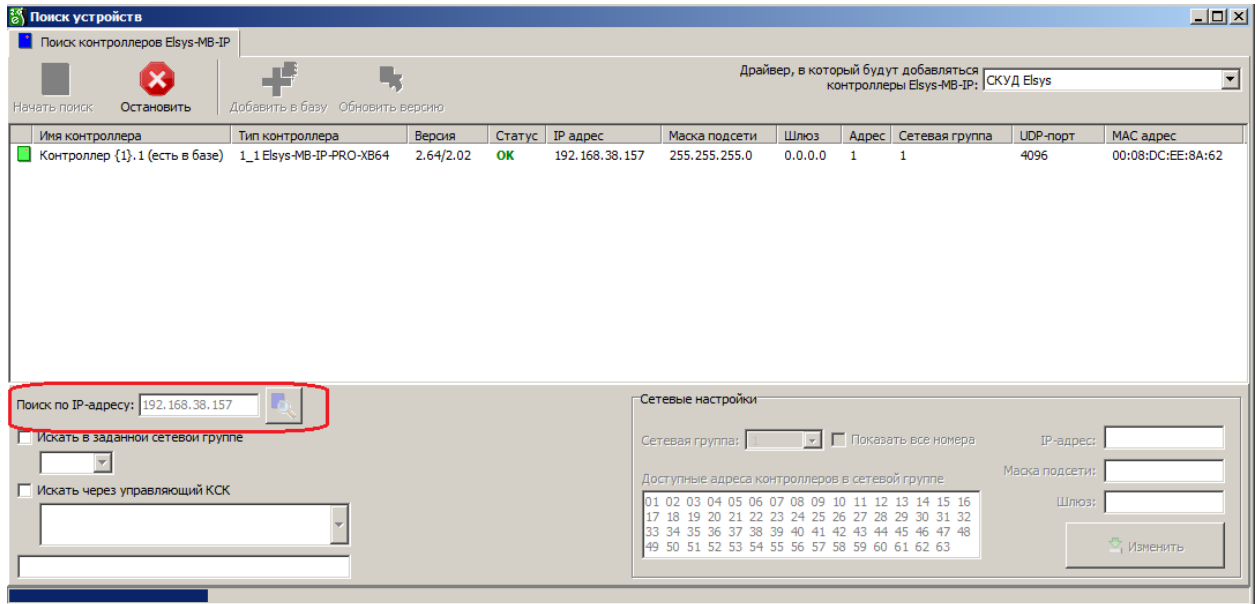


Рисунок 11 - Поиск контроллера Elsys-MB-IP по IP-адресу

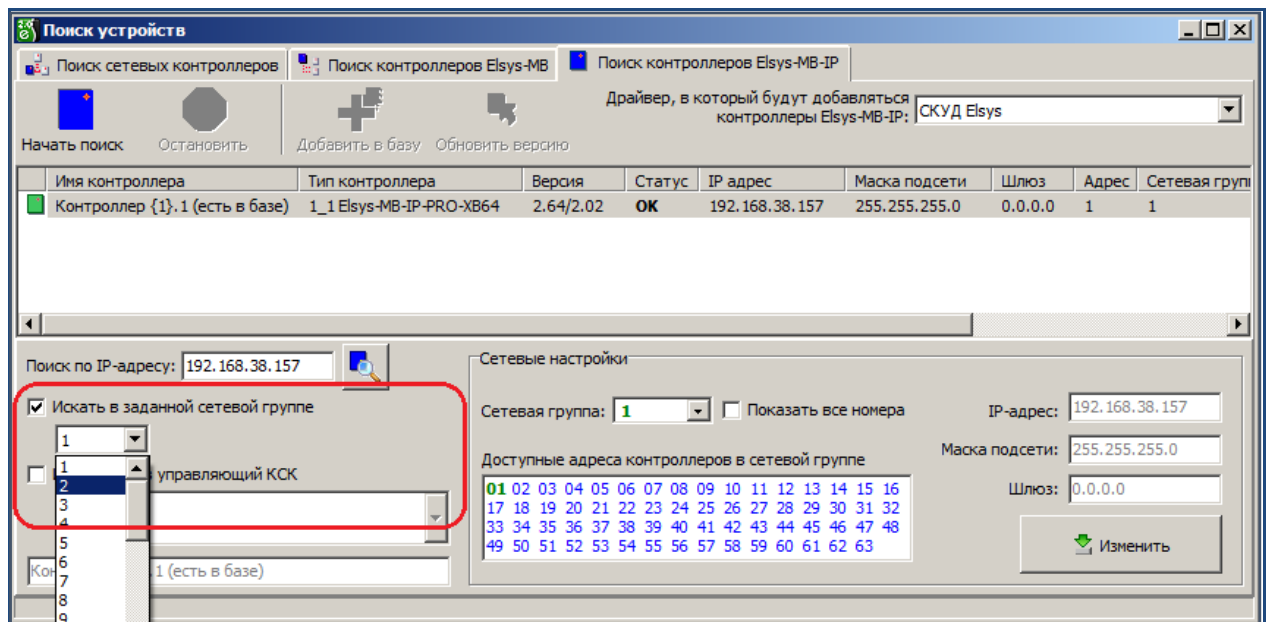


Рисунок 12 – Настройка поиска контроллеров в заданной сетевой группе

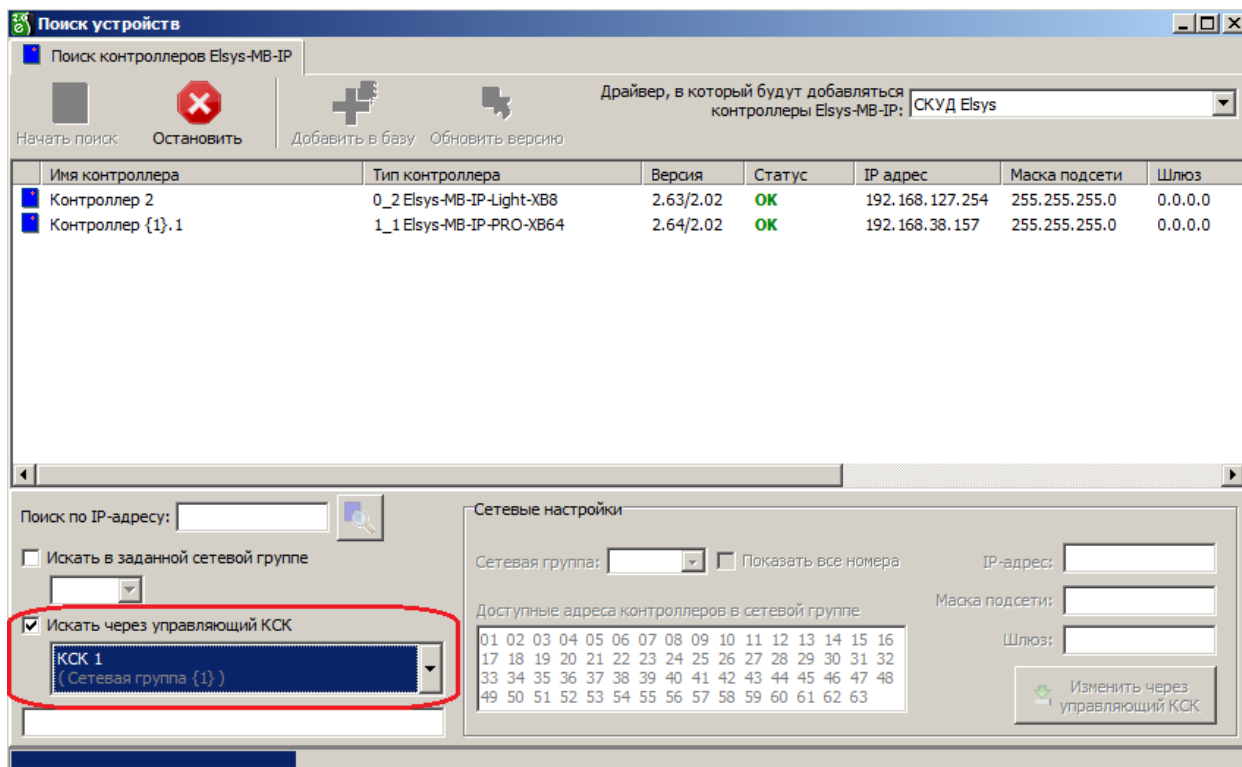


Рисунок 13 – Поиск контроллеров через управляющий КСК

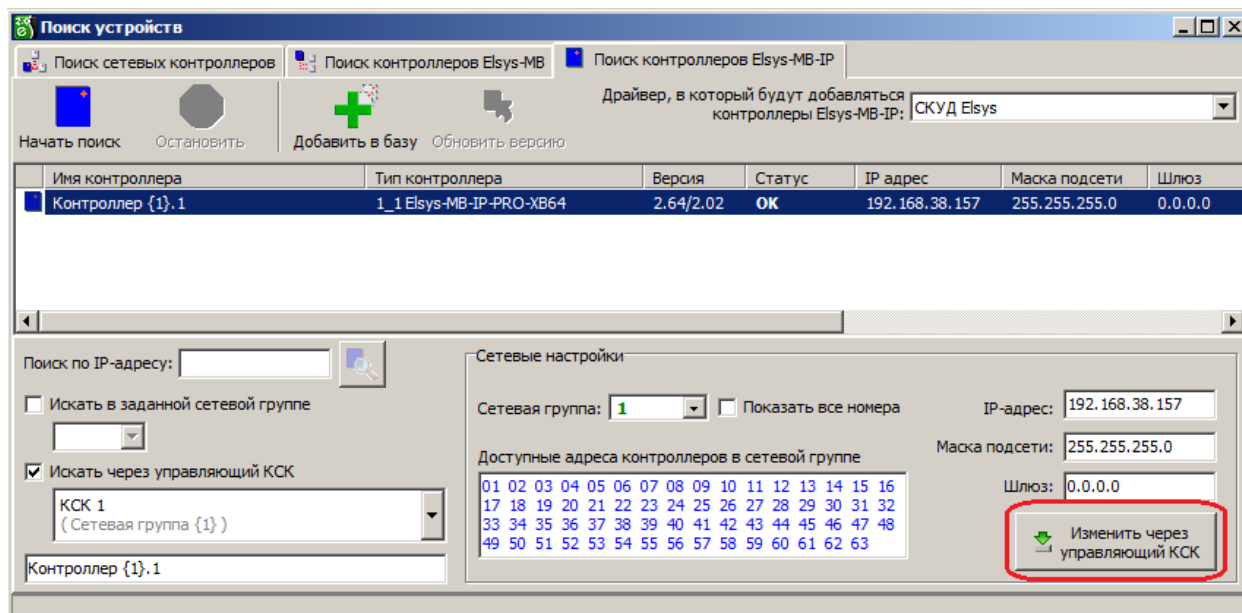


Рисунок 14 – Изменение сетевых настроек контроллера Elsys-MB-IP через управляющий КСК

Перед добавлением контроллера в базу данных можно изменить его наименование в целях более удобного представления информации (рисунок 15).

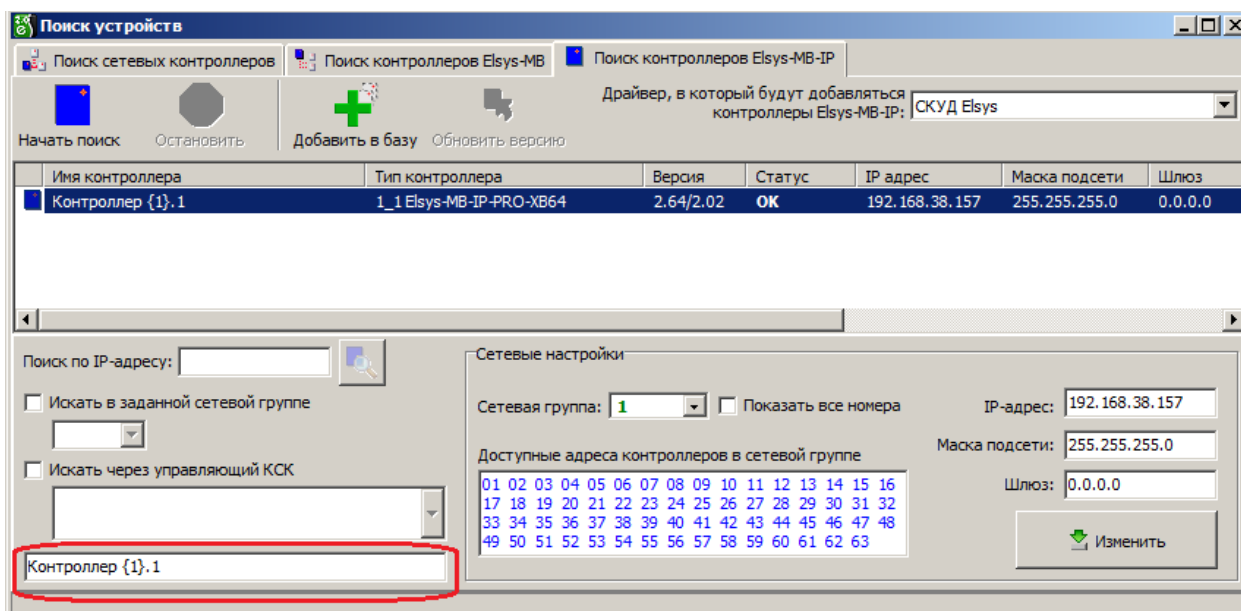


Рисунок 15 – Наименование контроллера Elsys-MB-IP

После того, как все настройки сделаны, контроллер может быть добавлен в базу данных кнопкой **«Добавить в базу»**.

Для добавляемого контроллера Elsys-MB-IP аналогично контроллерам Elsys-MB будет предложено выбрать готовую конфигурацию, совместимую с его вариантом исполнения (рисунок 7), либо пустую конфигурацию.

После выбора готовой конфигурации контроллер будет добавлен в базу данных и автоматически проинициализирован (рисунок 8), после чего он полностью готов к работе.

## 5 Конфигуратор оборудования

Конфигуратор оборудования вызывается с помощью кнопки **«Конфигурация оборудования»**, расположенной на ленте управления драйвером (рисунок 2).

В левой части окна конфигуратора (рисунок 16) находится дерево устройств, относящихся к драйверу «Бастион-2 – Elsys». В правой части окна находится окно просмотра, отображающее свойства выделенного узла.

Самый верхний уровень дерева устройств – драйверы «Бастион-2 – Elsys», присутствующие в системе. Узлы этого уровня формируются автоматически, после добавления драйвера, а имя узла совпадает с именем устройства, заданным при добавлении драйвера.

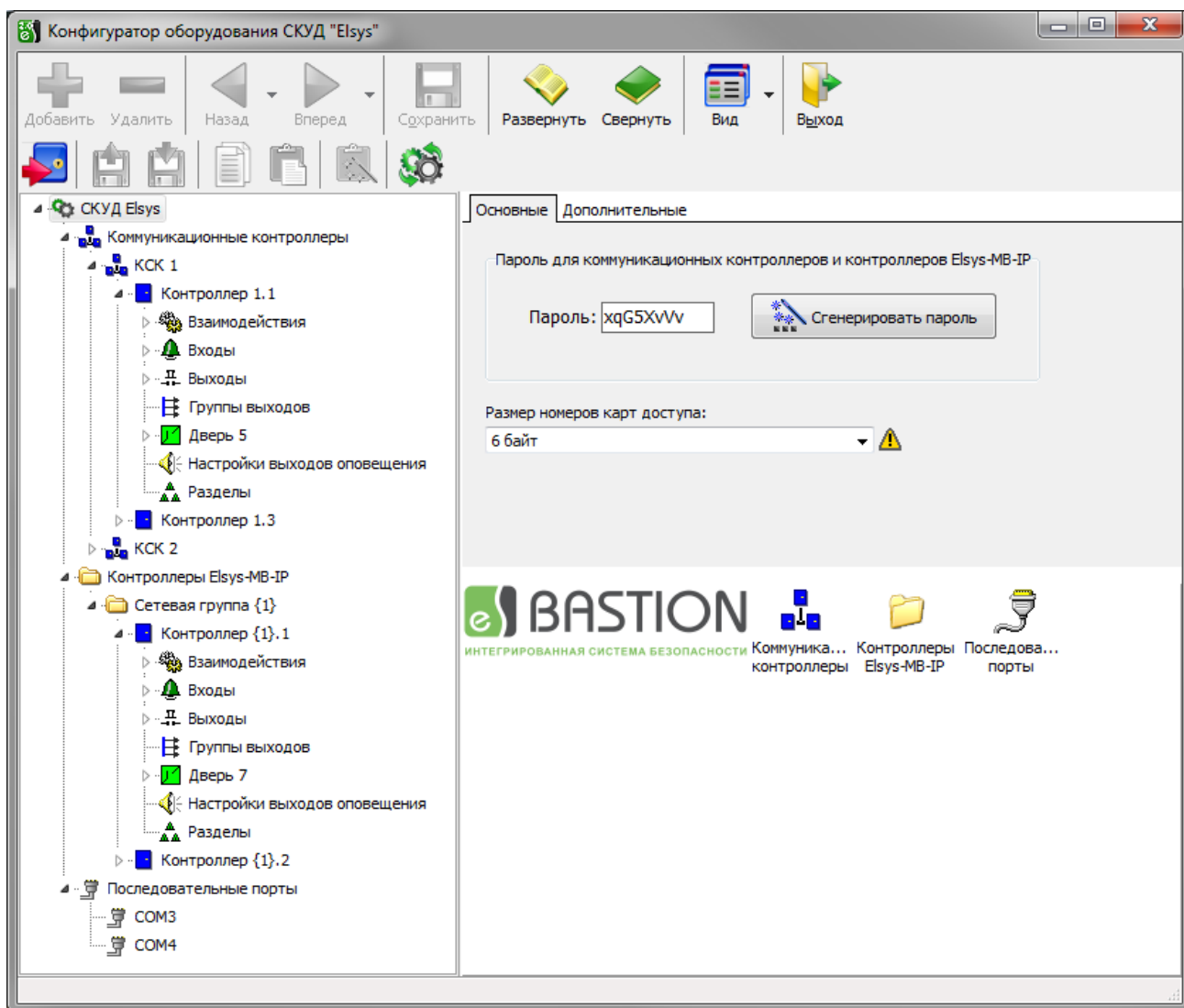








Рисунок 16 - Окно конфигуратора оборудования

На следующем уровне дерева устройств находятся узлы **«Коммуникационные контроллеры»**, **«Контроллеры Elsys-MB-IP»** и **«Последовательные порты»**, которые соответствуют трем возможным типам связи с контроллерами доступа: контроллеры доступа, подключенные через КСК, контроллеры доступа подключенные к компьютерной сети, контроллеры доступа подключенные непосредственно к COM-портам сервера оборудования Elsys.

В верхней части окна конфигуратора находятся две панели инструментов, назначение кнопок которых в таблицах 2 - 3.

Для настройки параметров устройства необходимо выбрать его в дереве устройств или произвести двойной щелчок по пиктограмме этого устройства в окне просмотра, при этом справа появится окно с параметрами выбранного устройства.








Таблица 2 - Назначение кнопок на панели управления

Кнопка	Наименование	Назначение
	«Добавить»	Добавляет новые устройства в конфигурацию. Функция также доступна из контекстного меню выбранного узла.
	«Удалить»	Удаляет существующие устройства из конфигурации (при этом удаляются также дочерние узлы). Функция также доступна из контекстного меню выбранного узла.
	«Назад»	Переход к предыдущему элементу в дереве устройств
	«Вперёд»	Переход к следующему элементу в дереве устройств
	«Сохранить»	Сохранить внесённые изменения
	«Развернуть»	Разворачивает все узлы дерева конфигурации
	«Свернуть»	Сворачивает все узлы дерева конфигурации
	«Вид»	Выбор стиля отображения дочерних устройств в окне просмотра
	«Выход»	<p>Выход из конфигуратора.</p> <p>При попытке выйти из конфигуратора без сохранения изменений появится окно с запросом: «Сохранить изменения в конфигураторе?».</p> <p>Для сохранения изменений параметров и выхода из конфигуратора следует выбрать «Да», для отмены сохранения изменений конфигурации – «Нет», для возврата к редактированию – «Отмена».</p>

Панель дополнительных средств драйвера, расположенная ниже, содержит кнопки, специфичные для драйвера «Бастион-2 – Elsys». Назначение кнопок на панели инструментов приведено в таблице 3.

Более подробная информация о работе с конфигурациями приведена в п. 5.7, а об инициализации контроллеров - в п. 7.

Таблица 3 - Назначение кнопок на панели дополнительных средств драйвера

Кнопка	Назначение
	Вызов формы инициализации оборудования
	Загрузка конфигурации панели из файла
	Сохранение конфигурации выбранной панели в файл. Активна, если выбранный узел в дереве устройств – панель
	Копирование конфигурации выбранной панели в буфер
	Вставка конфигурации из буфера
	Вставка готовой конфигурации панели
	Перезагрузка драйвера – перезагрузка всех данных из БД в динамическую библиотеку драйвера оборудования

## 5.1 Свойства драйвера «Бастион-2 – Elsys»

Окно свойств драйвера «Бастион-2 – Elsys» содержит две вкладки («**Основные**» и «**Дополнительные**») и список дочерних узлов дерева конфигурации (рисунок 17).

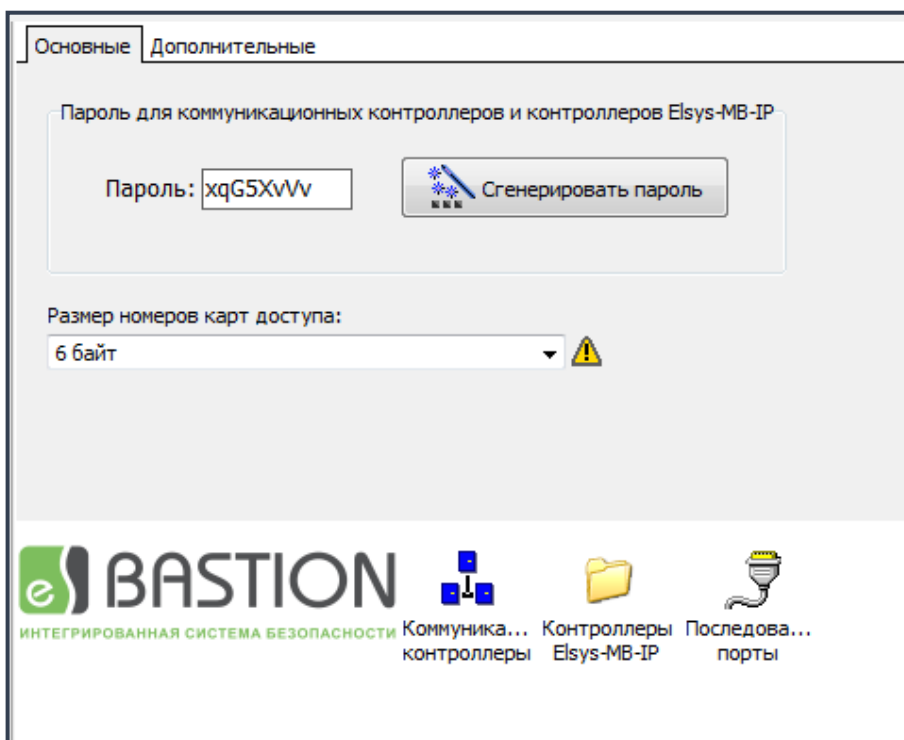


Рисунок 17 - Окно свойств драйвера «Бастион-2 – Elsys»

### 5.1.1 Вкладка «Основные»

С помощью группы управления «**Пароль для коммуникационных контроллеров и контроллеров Elsys-MB-IP**» можно задать ручную или автоматически сгенерировать



пароль для всех КСК и всех контроллеров Elsys-MB-IP, относящихся к выбранному экземпляру драйвера.

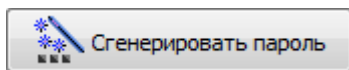
«**Пароль**» - настройка, задающая ключ шифрования, который используется драйвером оборудования при обмене сообщениями с КСК и контроллерами Elsys-MB-IP.

Связь с сетевыми контроллерами и контроллерами Elsys-MB-IP возможна лишь при совпадении паролей в драйвере и участвующих в обмене контроллерах.

По умолчанию сетевые контроллеры и контроллеры Elsys-MB-IP не имеют назначенного пароля и могут быть найдены поиском, независимо от того, какой пароль установлен в драйвере «Бастион-2 – Elsys».

Установка паролей в сетевых контроллерах и контроллерах Elsys-MB-IP происходит при записи сетевых настроек протокола IP. При записи сетевых настроек в контроллеры записывается пароль, используемый в драйвере «Бастион-2 – Elsys».

Пароль должен содержать 8 алфавитно-цифровых символов (допускается использовать только цифры и латинские прописные и строчные буквы).



Кнопка генерирует по псевдослучайному закону новый пароль.

Изменённый пароль будет передан в контроллеры при сохранении в базу данных.

**Внимание!** Если с КСК или с контроллером Elsys-MB IP связь отсутствует (даже если он включен и подключен к ЛВС), то пароль в него записан не будет, что приведет к полной потере связи с ним в дальнейшем, в том числе при поиске оборудования. При возникновении такой ситуации необходимо установить пароль по умолчанию, выполнив аппаратный сброс настроек сетевого контроллера или контроллера Elsys-MB-IP.

Если на момент сохранения будет отсутствовать связь хотя бы с одним из контроллеров, то будет открыто диалоговое окно с соответствующим предупреждением (рисунок 18), позволяющее отказаться от сохранения в базу данных.

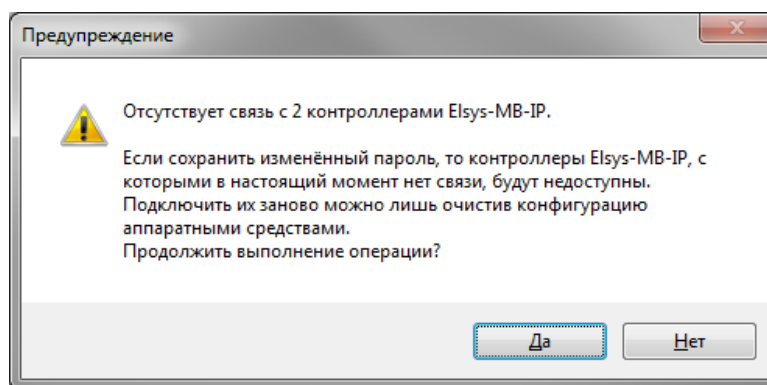


Рисунок 18 - Предупреждение при сохранении в базу данных

«**Размер номеров карт доступа**» - настройка, задающая размер номеров карт доступа в байтах в драйвере. Возможные значения размера номера карт: 3 байта и 6 байт (рисунок 19).

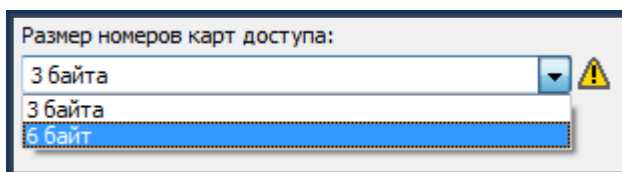


Рисунок 19 - Установка размера номера карт в драйвере

В ПО «Бастион-2» используется размер номеров карт 6 байт, для совместимости с предыдущими версиями ПО «Бастион», а также для работы с контроллерами старых версий, в которых не поддерживаются 6-байтные номера карт, в драйвере может быть установлен размер номеров карт 3 байта. Для работы в режиме работы с 3-байтными номерами карт в драйвере реализован механизм восстановления полного 6-байтного номера по его 3-байтному значению.

**Внимание!** После изменения размера номеров карт доступа требуется выполнить полную инициализацию всех контроллеров, относящихся к драйверу.

### 5.1.2 Вкладка «Дополнительные»

На рисунке 20 показана вкладка с дополнительными настройками драйвера.

Если включена опция «**Автоматически инициализировать контроллеры**», в заданное время, которое определяется параметром «**Время автоматической инициализации**», будут инициализироваться уровни доступа, временные блоки, праздники, карты доступа во всех контроллерах, где включена опция «**Инициализировать с настройками драйвера**». Кроме того, настройку автоматической инициализации можно задать для каждого контроллера индивидуально (п. 5.5.2 , рисунок 41).

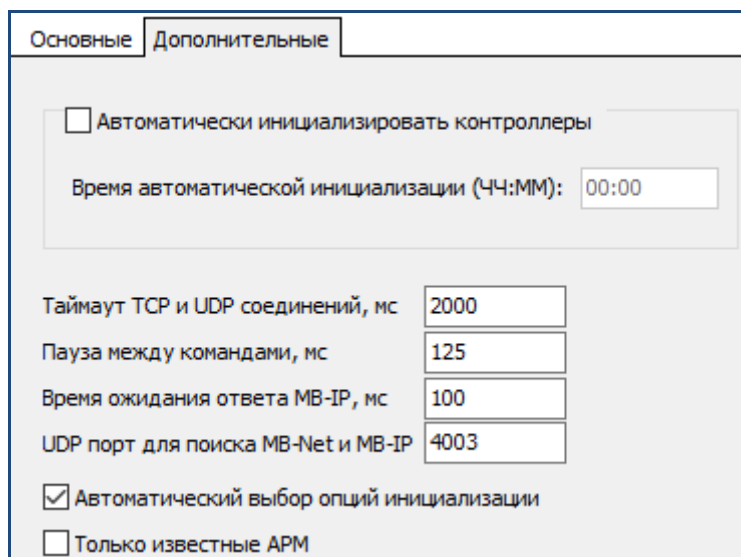


Рисунок 20- Окно свойств драйвера «Бастион-2 – Elsys», вкладка «Дополнительные»

«**Таймаут TCP и UDP соединений**» - время, отводимое на установление соединения с КСК или контроллером. После истечения указанного времени выполняется повторная попытка соединения с устройством. При недостаточном таймауте могут наблюдаться кратковременные потери связи с устройствами, при излишне длительном – с задержкой определяется потеря связи с устройством, замедляется повторное установление связи после ошибок связи.

«**Пауза между командами**» - при отсутствии команд в очереди, КСК опрашивается с вышеуказанным периодом. При уменьшении параметра, увеличивается скорость обработки команд и событий, но возникает дополнительная нагрузка на сеть и процессор. Без необходимости изменять не следует.

«**Время ожидания ответа от MB-IP**» - По истечении указанного времени после отправки команды для MB-IP и отсутствии ответа от последнего, драйвер переходит к опросу следующего MB-IP. При уменьшении времени возможны кратковременные потери связи с MB-IP, при увеличении – опрос MB-IP будет существенно замедляться при отсутствии связи с одним или несколькими из них.

«**UDP порт для поиска MB-Net и MB-IP**» - при недоступности порта по умолчанию (4003), можно указать номер другого порта или 0 – для динамического выбора порта из доступных.

«**Автоматический выбор опций инициализации**» - в окне инициализации оборудования автоматически устанавливаются опции, которые следует инициализировать. На системах с большим количеством оборудования инициализация всего оборудования может занимать длительное время. и поэтому производится по частям. Отключение вышеуказанной опции позволяет самостоятельно выбирать инициализируемое оборудование, избегая ошибочного запуска инициализации всей системы.

«**Только известные АРМ**» - уменьшает нагрузку на сеть за счёт отправки информации от драйвера только рабочим станциям, добавленным в список в окне «Сеть». Актуально для систем с несколькими десятками рабочих станций. При включении опции, на рабочих станциях, не добавленных в список «Сеть», не будет работать проверка связи, конфигурации, поиск, инициализация.

## 5.2 Настройка сетевых контроллеров Elsys-MB-Net

Добавление сетевых контроллеров Elsys-MB-Net в базу данных во многих случаях (в особенности, при первом знакомстве с системой) целесообразно выполнять из окна «Поиск оборудования» (функция «Поиск оборудования» описана в п. 4), сразу после обнаружения и начальной настройки подключенного оборудования. Это позволяет избежать ошибок, связанных с несоответствием характеристик оборудования (номер, версия, сетевые настройки и т. д.).

Также для первичной настройки контроллеров Elsys-MB-Net можно воспользоваться утилитой «MBNetProg.exe».

Сетевые контроллеры могут быть добавлены в базу данных непосредственно в конфигураторе оборудования, однако в дальнейшем потребуется выполнить их поиск, начальную настройку и привести в полное соответствие реальные характеристики оборудования и настройки в базе данных.

Для добавления сетевого контроллера Elsys-MB-Net в базу данных (рисунок 21) следует выделить узел «**Коммуникационные контроллеры**» в дереве устройств и правой кнопкой мыши вызвать контекстное меню, в котором выбрать пункт «**Добавить**», затем пункт «**Коммуникационный контроллер**». Либо, выделив узел «**Коммуникационные**

контроллеры» в дереве устройств, нажать кнопку «Добавить» на панели инструментов (рисунок 22).

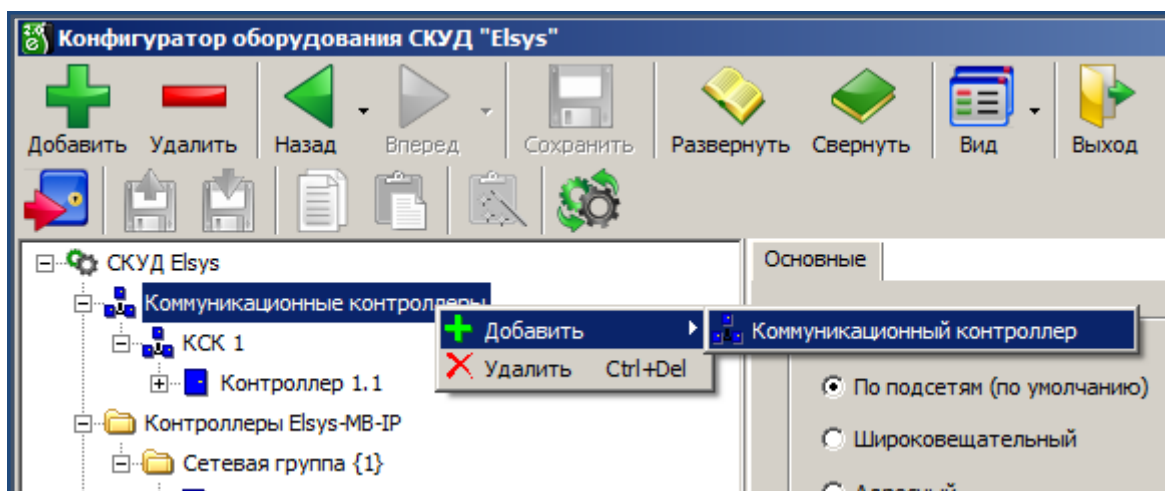


Рисунок 21 - Добавление сетевого контроллера с помощью контекстного меню дерева конфигурации

Окно свойств сетевого контроллера содержит вкладки с основными (вкладка «Основные») и дополнительными (вкладка «Дополнительные») настройками и список подключенных контроллеров доступа (рисунок 23).

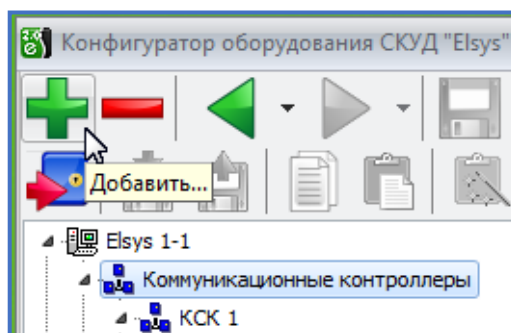


Рисунок 22 - Добавление сетевого контроллера с помощью панели инструментов

Основные
Дополнительные

Наименование КСК:

Входит в сетевую группу:

Исключён из опроса

Номер:

Версия:

**Настройки для линии связи RS-485 сетевого контроллера**

Глобальный контроль последовательности прохода

Глобальный antipassback выключен.

Усиленный antipassback

**Использование контроля последовательности прохода в контроллерах доступа**

№	Наименование контроллера	Контроль последовательности прохода
1	Контроллер 1.1	Глобальный antipassback выкл.
2	Контроллер 1.3	Глобальный antipassback выкл.

Скорость обмена, бит/с:

Режим обмена:  MASTER - SLAVE  MULTIMASTER

**Настройки для локальной сети**

IP Адрес:

Маска подсети:

Шлюз:

Не проверять исправность областей контроля

Транслировать межконтроллерные взаимодействия в другие линии связи

Контроллер  
1.1

Контроллер  
1.3

Рисунок 23 - Окно свойств сетевого контроллера

### 5.2.1 Вкладка «Основные»


«**Наименование КСК**» - наименование сетевого контроллера, которое можно изменить в целях более удобного представления информации.

«**Номер**» - уникальный идентификатор сетевого контроллера. Может принимать значения от 1 до 255.

«**Версия**» - версия встроенного управляющего программного обеспечения сетевого контроллера Elsys-MB-Net (версия прошивки). Версия прибора анализируется драйвером при работе с контроллером и должна соответствовать реальному значению, прочитанному из контроллера.

**Внимание!** Неправильное задание номера версии может вызвать некорректную работу системы с оборудованием.

Список всех известных версий прошивок контроллеров хранится в динамической библиотеке драйвера оборудования Elsys. В конфигураторе драйвера список версий прошивки (рисунок 24) включает список всех известных версий прошивки и версий прошивок сетевых контроллеров из БД. Несоответствие версии из списка реальному значению отображается цветом фона. На сером фоне отображаются версии, которые меньше реальной версии контроллера, на желтом фоне отображаются версии, которые старше реальной версии контроллера, на красном фоне – номера неизвестных версий прошивки.

При выборе несоответствующей версии прошивки КСК отображается значком с восклицательным знаком , а метка поля со списком версий отображается в виде гиперссылки красного цвета (рисунок 25), с помощью которой можно получить информацию о реальной версии контроллера (рисунок 26) и, по возможности, установить корректное значение.

При добавлении КСК из конфигуратора реальная версия прошивки неизвестна, поэтому метка списка версий также отображается в виде гиперссылки красного цвета.

Обновление реальных значений версий прошивки КСК выполняется автоматически после установления связи и после выполнения поиска контроллеров.

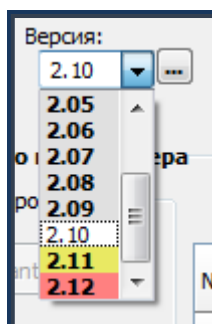


Рисунок 24 – Список версий прошивки в конфигураторе

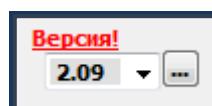


Рисунок 25 – Список версий прошивки в конфигураторе

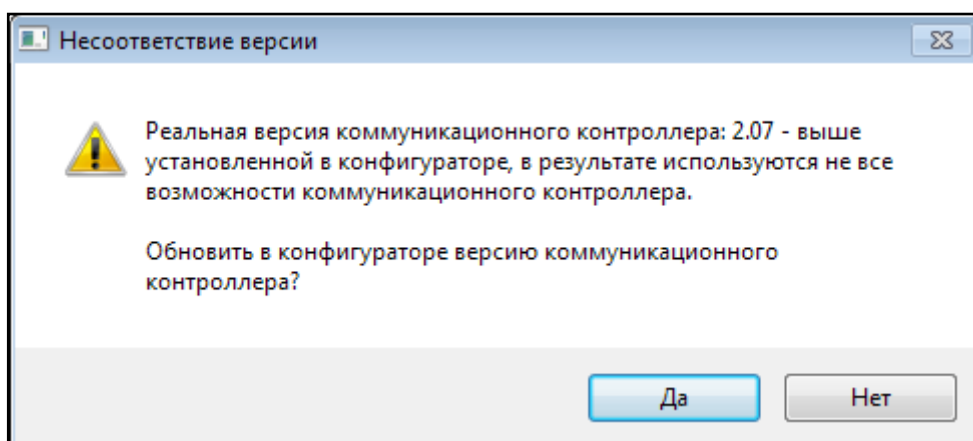



Рисунок 26 – Список версий прошивки в конфигураторе

**«Входит в сетевую группу»** - этот параметр указывает на принадлежность КСК к одной из сетевых групп контроллеров Esys-MB-IP. Входящий в сетевую группу КСК обеспечивает обмен данными с контроллерами других сетевых групп и КСК. Для включения КСК в сетевую группу необходимо ее выбрать в выпадающем списке, при этом положение узла КСК в дереве конфигурации не изменится, а в изображении иконки КСК появится значок сетевой группы: , для индикации управляющего КСК. Включение КСК в сетевую группу, как правило, требуется при включенной функции **«Глобальный контроль последовательности прохода»**, когда необходимо обеспечить обмен данными контроллеров сетевой группы с другими КСК (см. п. 6.2).

**«Исключён из опроса»** - при включении этой опции драйвер перестаёт опрашивать КСК, при выключении опции драйвер начинает опрашивать КСК. Опция может быть полезна при временном отсутствии КСК в линии связи, для оптимизации процесса опроса, или в других случаях, когда не требуется получать информацию от данного КСК и всех подключенных к нему контроллеров доступа.

***Внимание!** При включении опроса потребуются полная инициализация КСК и всех подключенных к нему контроллеров доступа.*

**«Не проверять исправность областей контроля»** - настройка, задающая алгоритм работы функции **«Глобальный контроль последовательности прохода»** при потере связи с отдельными контроллерами. Настройка загружается в сетевой контроллер Esys-MB-Net и подключенные к нему контроллеры доступа Esys-MB при инициализации оборудования.

Если используются контроллеры Esys-MB версий 2.60 и выше, а также контроллеры Esys-MB-Net версий 2.08 и выше, настройка загружается в контроллеры автоматически, после выхода из конфигуратора.

**«Транслировать межконтроллерные взаимодействия в другие линии связи»** - настройка, позволяющая включать (отключать) передачу широковещательных сообщений от контроллеров доступа, подключенных к данному КСК, контроллерам, подключенных к другим КСК. Использование настройки описано в п. 9.1.5.

#### 5.2.1.1 Настройки для линии связи RS-485 сетевого контроллера

**«Глобальный контроль последовательности прохода»** - группа элементов управления, которая позволяет включать и выключать режим глобального контроля последовательности прохода в сетевом контроллере, а также выводит текстовую информацию о корректности его настройки. Настройка глобального контроля последовательности прохода подробно описана в п. 6.2.

**«Усиленный antipassback»** – режим, обеспечивающий дополнительную защиту от несанкционированного доступа. Описание настройки приведено в п. 6.5. Данный режим возможен для контроллеров Esys-MB старших моделей (Pro, Standard, Light, Pro4) версий 2.60 и выше. КСК Esys-MB-Net, обеспечивающие обмен данными, должны иметь версию не ниже 2.08.

**«Использование контроля последовательности прохода в контроллерах доступа»** - это информационная таблица, которая служит для отображения использования настройки



«Контроль последовательности прохода» в контроллерах доступа, подключенных к данному КСК.

**«Скорость обмена»** - скорость обмена информацией (в бит/с) с сетью контроллеров. Допустимые значения – 4800, 9600, 19200, 38400, 57600, 115200 бит/с. Немедленно после выхода из конфигуратора оборудования настройка загружается в сетевой контроллер Elsys-MB-Net и подключенные к нему контроллеры Elsys-MB.

**«Режим обмена»** - настройка задает режим обмена сетевого контроллера с другими КСК.

Режим **MASTER-SLAVE**, используется при начальной настройке системы и может использоваться в дальнейшем, если не требуется использование функции глобального контроля последовательности прохода. Сетевой контроллер в этом режиме является ведущим, и опрашивает подключенные к нему контроллеры доступа по очереди. Контроллеры доступа в этом режиме не обмениваются информацией друг с другом.

Режим **MULTIMASTER**, используется, если необходимо использование функции глобального контроля последовательности прохода. В режиме MULTIMASTER подключенные к КСК контроллеры доступа обмениваются информацией между собой, при этом возможность поиска контроллеров доступа, подключенных к КСК, отсутствует.

Переключение режима обмена происходит после выхода из конфигуратора оборудования. В этот момент все подключенные к КСК контроллеры доступа обязательно должны находиться на линии связи.

#### 5.2.1.2 Настройки для локальной сети

**«IP-адрес»** - IP-адрес сетевого контроллера в ЛВС.

**«Маска подсети»** - маска подсети для сетевого контроллера.

**«Шлюз»** - IP-адрес шлюза в ЛВС.

#### 5.2.2 Вкладка «Дополнительные»

Окно дополнительных настроек сетевого контроллера включает дополнительные настройки для локальной сети и сети RS-485 (рисунок 27).

##### 5.2.2.1 Дополнительные настройки для локальной сети

Параметры **«Задержка передачи пакета данных»** и **«Время ожидания ответа»** предназначены для настройки временных характеристик обмена информацией между сетевыми контроллерами по протоколу UDP. Установки по умолчанию подходят для большинства применений, и без необходимости их изменять не следует.



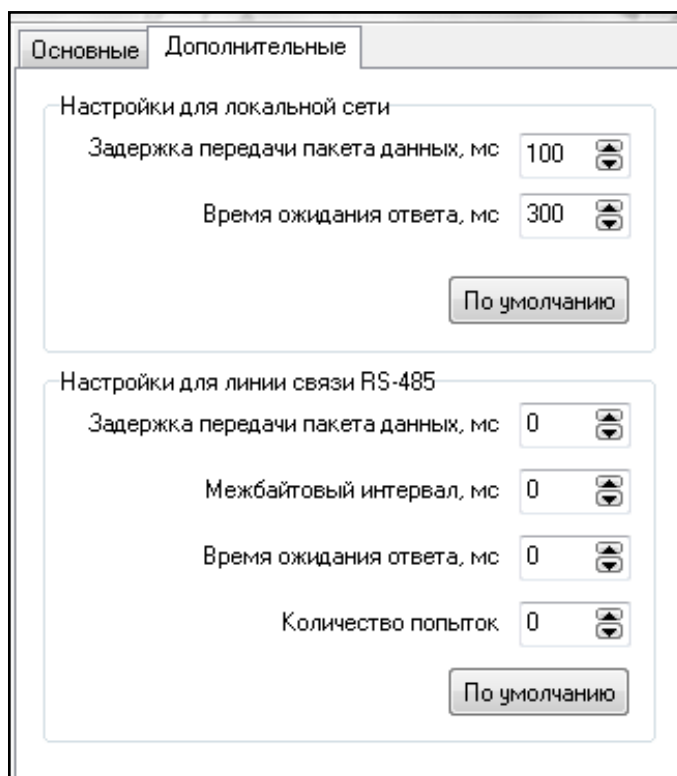
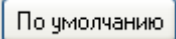


Рисунок 27 – дополнительные параметры КСК

Кнопка  устанавливает дополнительные настройки для локальной сети равными значениям по умолчанию.

#### 5.2.2.2 Дополнительные настройки для линии связи RS-485

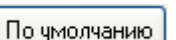
Группа настроек предназначена для адаптации к различным сложным условиям в линии RS-485 сетевого контроллера (например, при удлинении канала связи с использованием конвертеров интерфейсов «RS-485/оптоволокно», использовании радиоканала, большом уровне помех и т. д.). Эти настройки без необходимости изменять не следует.

Настройка **«Задержка передачи пакета данных»** (0-255 мс, по умолчанию – 0) предназначена для формирования задержки очередной информационной посылки сетевого контроллера.

Настройки **«Межбайтовый интервал»** и **«Время ожидания ответа»** задают таймауты для операции чтения в режиме MASTER-SLAVE.

Настройка **«Количество попыток»** задаёт критерий для формирования сообщения «Потеря связи» в режиме MASTER-SLAVE – число неудачных попыток опроса контроллера подряд.

При этом, если заданы нулевые значения, время ожидания ответа составляет 150 мс, межбайтовый интервал зависит от скорости обмена (на 38400 бит/с составляет 10 мс), а количество попыток равно шести.

Кнопка  устанавливает значения параметров **«Задержка передачи пакета данных»**, **«Межбайтовый интервал»**, **«Время ожидания ответа»**, **«Количество попыток»** на заданные по умолчанию нулевые значения.

### 5.3 Настройка сетевых групп контроллеров Elsys-MB-IP

Добавление сетевых групп происходит автоматически при добавлении найденных контроллеров Elsys-MB-IP из окна поиска (см. п. 4.3).

Сетевые группы могут быть добавлены в базу данных непосредственно в конфигураторе оборудования с целью добавления в них контроллеров Elsys-MB-IP.

Для добавления сетевой группы в базу данных следует выделить узел **«Контроллеры Elsys-MB-IP»** в дереве устройств и правой кнопкой мыши вызвать контекстное меню, в котором выбрать пункт **«Добавить»**, затем пункт **«Сетевую группу»** (рисунок 28).

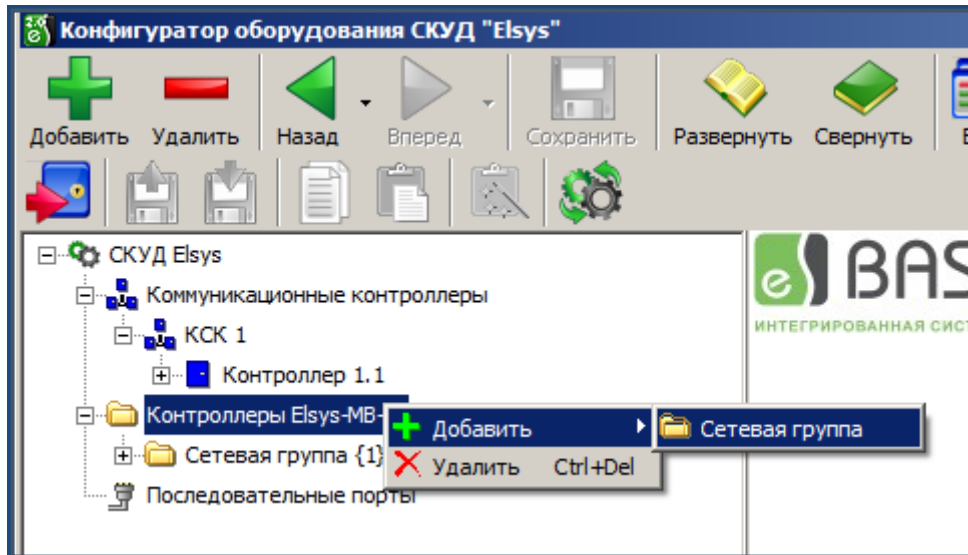


Рисунок 28 – Добавление сетевой группы

Либо, выделив узел **«Контроллеры Elsys-MB-IP»** в дереве устройств, нажать кнопку **«Добавить»** на панели инструментов.

Окно свойств сетевой группы представлено на рисунке 29.

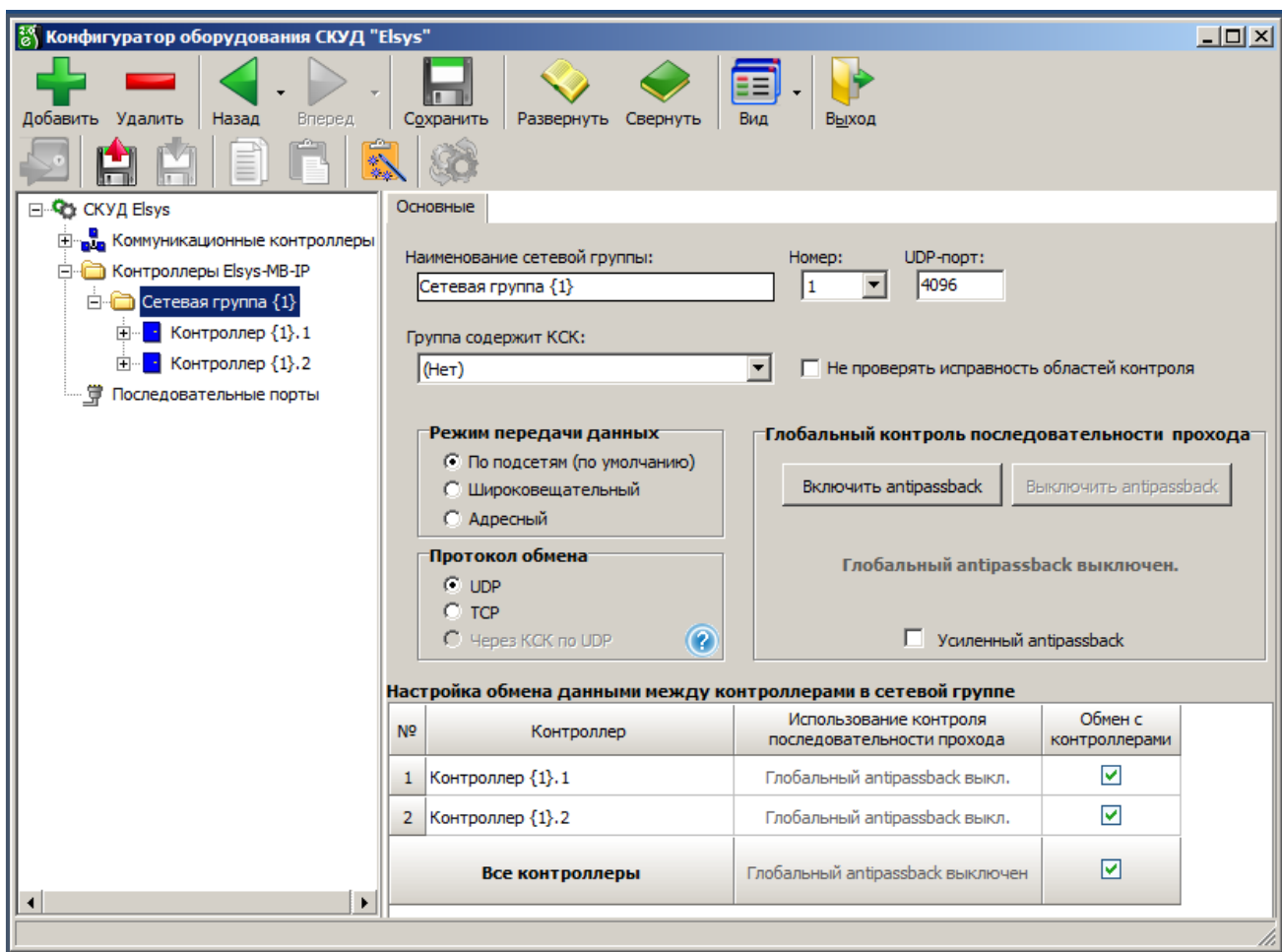


Рисунок 29 – Окно свойств сетевой группы

«**Наименование сетевой группы**» - наименование сетевой группы, которое можно изменить в целях более удобного представления информации.

«**Номер**» - уникальный номер сетевой группы. Может принимать значения от 1 до 254.

«**UDP-порт**» - это номер UDP-порта, который используется контроллерами сетевой группы для обмена сообщениями по протоколу UDP.

«**Группа содержит КСК:**» - эта настройка содержит ссылку на управляющий КСК, который обеспечивает обмен данными с другими сетевыми группами и КСК. Включение КСК в сетевую группу, как правило, необходимо при включенной функции «**Глобальный контроль последовательности прохода**» (см. п. 6.2).

«**Не проверять исправность областей контроля**» - настройка, задающая алгоритм работы функции «**Глобальный контроль последовательности прохода**» при потере связи с отдельными контроллерами. Настройка загружается в контроллеры Elsys-MB-IP автоматически при выходе из конфигуратора.

### 5.3.1 Режим передачи данных

«**Режим передачи данных**» - режим обмена информацией по протоколу UDP между контроллерами Elsys-MB-IP в сетевой группе. Настройка может принимать три значения – «По подсетям (по умолчанию)», «Широковещательный» и «Адресный».

**«По подсетям (по умолчанию)»** - режим передачи данных, в котором контроллеры сетевой группы обмениваются пакетами с адресом подсети, например, 192.168.1.255.

**«Широковещательный»** - режим передачи данных, в котором контроллеры сетевой группы при обмене сообщениями отправляют широковещательные пакеты.

**«Адресный»** - режим передачи данных, в котором контроллеры сетевой группы при обмене сообщениями отправляют адресные широковещательные пакеты.

Если контроллеры сетевой группы участвуют в работе функции **«Глобальный контроль последовательности прохода»**, рекомендуется установить значение **«По подсетям»**. Два других режима – **«Широковещательный»** и **«Адресный»** – следует использовать в исключительных случаях, после предварительных консультаций с разработчиками.

### 5.3.2 Протокол обмена

Протокол обмена задаёт режим работы IP-контроллеров сетевой группы.

**«UDP»** - это режим опроса Elsys-IP непосредственно с компьютером по протоколу UDP. Поддерживается всеми версиями Elsys-IP.

*Условия применения:* обычная локальная сеть предприятия, где минимальна задержка доставки пакетов и нет препятствий для прохождения UDP-пакетов.

**«TCP»** - это режим опроса Elsys-IP непосредственно с компьютером по протоколу TCP. Поддерживается модулями Elsys-IP, имеющими версию начиная с 2.02.

*Условия применения:* целесообразно использовать для подключенных удалённо, в том числе через Internet, модулей Elsys-IP, а также в иных случаях, когда есть сложности с прохождением UDP-пакетов. Режим рекомендуется использовать при удалённом подключении небольших объектов (1 – 2 точки доступа).

**«Через КСК по UDP»** - это режим опроса модулей Elsys-IP по протоколу UDP через КСК Elsys-MB-Net. Для работы этого режима необходимо, чтобы версия Elsys-MB-Net была не ниже 2.10. Версии модулей Elsys-IP могут быть любыми. КСК Elsys-MB-Net должен быть включен в обслуживаемую им сетевую группу.

*Ограничения:* в этом режиме недоступен обмен информацией с другими КСК, который необходим для обеспечения антипассбэка и межконтроллерных взаимодействий.

*Условия применения:* режим оптимален, если необходимо подключить удалённо через КСК Elsys-MB-Net, по протоколу TCP/IP, группы контроллеров (подключенных к КСК как через Elsys-IP, так и по RS-485), с использованием минимально возможного числа TCP/IP соединений (по одному TCP/IP соединению на каждый удалённый объект). Режим рекомендуется использовать, если необходимо организовать удалённое подключение к серверу оборудования СКУД крупного объекта (несколько точек доступа).

### 5.3.3 Глобальный контроль последовательности прохода

«Глобальный контроль последовательности прохода» - группа элементов управления, которая позволяет включать и выключать режим глобального контроля последовательности прохода в сетевой группе, а также выводит текстовую информацию о корректности его настройки. Более подробно настройка глобального контроля последовательности прохода описана в п. 6.2.

«Усиленный antipassback» - режим, обеспечивающий дополнительную защиту от несанкционированного доступа, после редактирования данная настройка загружается в контроллеры Elsys-MB-IP автоматически при выходе из конфигуратора. Подробное описание настройки приведено в п. 6.5.

### 5.3.4 Настройка обмена данными между контроллерами в сетевой группе

«Настройка обмена данными между контроллерами в сетевой группе» - таблица, которая служит для отображения настройки контроля последовательности прохода в контроллерах сетевой группы, а также для включения(выключения) обмена сообщениями контроллера сетевой группы с другими контроллерами в сетевой группе.

## 5.4 Настройка линий связи RS-485, подключенных к COM-порту

Окно с настройками для линий связи RS-485, подключенных к последовательным портам сервера оборудования, открывается при выборе в дереве конфигурации узла соответствующего COM-порта (рисунок 16).

Окно свойств линии связи COM-порта содержит две вкладки с параметрами: «Основные» (рисунок 30), «Дополнительные» (рисунок 31), а также список контроллеров доступа, подключенных к данной линии связи.

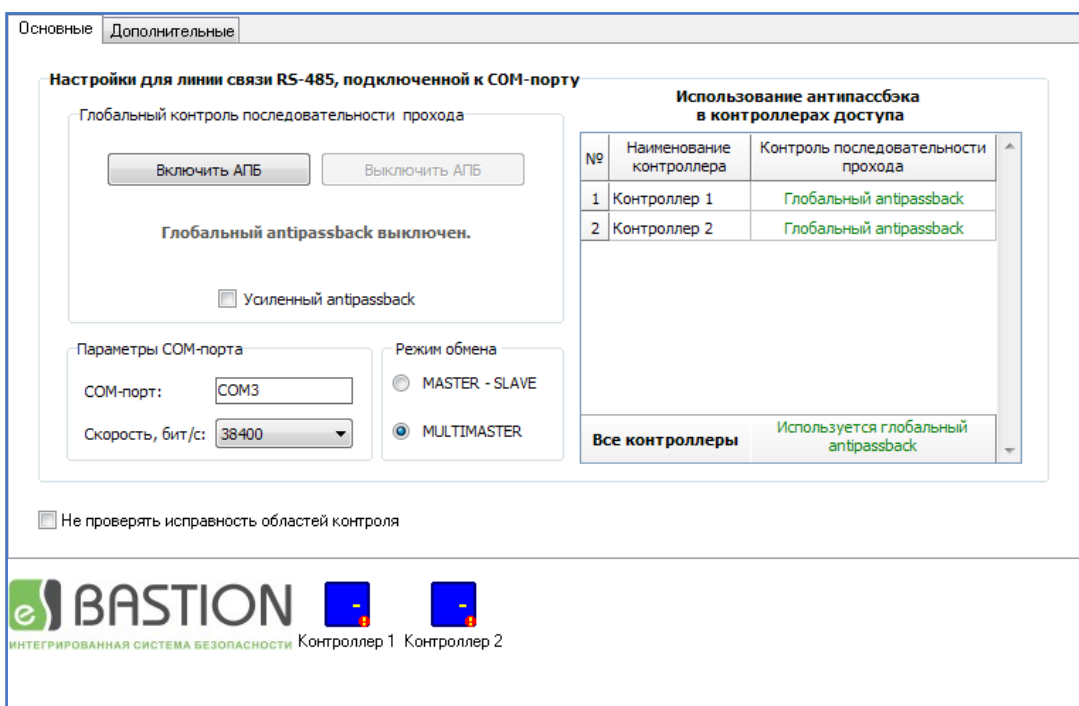


Рисунок 30 – Настройка линий связи RS-485, подключенных к COM-порту (вкладка «Основные»)

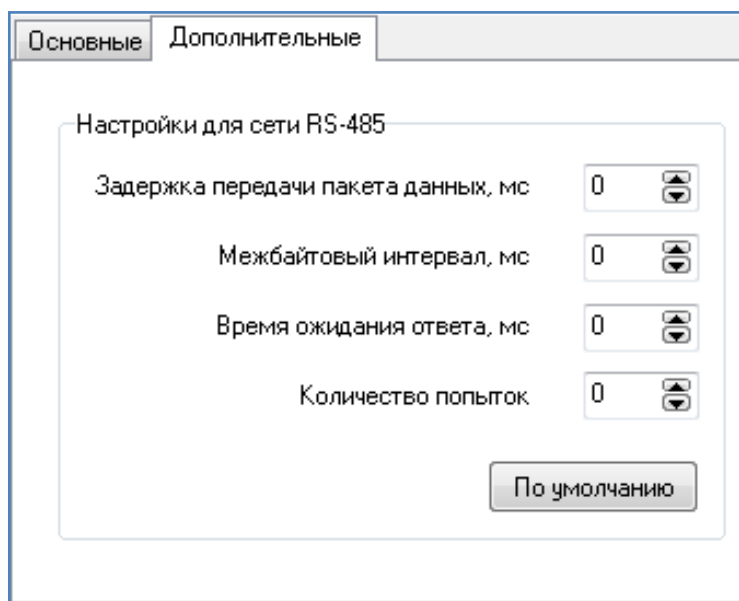


Рисунок 31 – Настройка линий связи RS-485, подключенных к COM-порту (вкладка «Дополнительные»)

#### 5.4.1 Вкладка «Основные»

Параметры линии связи COM-порта на вкладке «Основные» (рисунок 30) по смыслу аналогичные одноименным параметрам линии связи RS-485 сетевого контроллера (п. 5.2.1, рисунок 23).

**«Глобальный контроль последовательности прохода»** - группа элементов управления, которая позволяет включать и выключать режим глобального контроля последовательности прохода в линии связи COM - порта, а также выводит текстовую информацию о корректности его настройки. Настройка глобального контроля последовательности прохода подробно описана в п. 6.5.

**«Усиленный antipassback»** – режим, обеспечивающий дополнительную защиту от несанкционированного доступа. Описание настройки приведено в п. 6.5. Данный режим возможен для контроллеров Elsys-MB старших моделей (Pro, Standard, Light, Pro4) версий 2.60 и выше.

**«Использование контроля последовательности прохода в контроллерах доступа»** - это информационная таблица, которая служит для отображения использования настройки «Контроль последовательности прохода» в контроллерах доступа, подключенных к COM-порту.

**«Параметры COM-порта»** - группа параметров служит для отображения и настройки свойств последовательного порта, к которому подключена линия связи RS-485.

**«COM-порт»** - наименование последовательного порта, настройка является информационной и не доступна для редактирования.

**«Скорость обмена»** - скорость обмена информацией (в бит/с) с сетью контроллеров. Допустимые значения – 4800, 9600, 19200, 38400, 57600, 115200 бит/с. Немедленно после

выхода из конфигуратора оборудования настройка загружается в контроллеры Elsys-MB, подключенные к COM-порту.

**«Режим обмена»** - настройка задает режим обмена в линии RS-485.

Режим **MASTER-SLAVE**, используется при начальной настройке системы и может использоваться в дальнейшем, если не требуется использование функции глобального контроля последовательности прохода. Сервер оборудования в этом режиме является ведущим, и опрашивает подключенные к нему через COM-порт контроллеры доступа по очереди. Контроллеры доступа в этом режиме не обмениваются информацией друг с другом.

Режим **MULTIMASTER**, используется, если необходимо использование функции глобального контроля последовательности прохода. В режиме MULTIMASTER подключенные к COM-порту сервера оборудования контроллеры обмениваются информацией между собой, при этом возможность поиска контроллеров доступа, подключенных к COM-порту сервера оборудования, отсутствует.

Переключение режима обмена происходит после выхода из конфигуратора оборудования. В этот момент все подключенные через COM-порт к линии RS-485 контроллеры доступа обязательно должны находиться на линии связи.

#### 5.4.2 Вкладка «Дополнительные»

Группа дополнительных настроек линии RS-485 на вкладке «Дополнительные» (рисунок 31) предназначена для адаптации к различным сложным условиям в линии RS-485 (например, при удлинении канала связи с использованием конвертеров интерфейсов «RS-485/оптоволокно», использовании радиоканала, большом уровне помех и т. д.). Эти настройки без необходимости изменять не следует.

Настройки аналогичны одноименным настройкам для линии RS-485 сетевого контроллера (п. 5.2.2.2, рисунок 27).

#### 5.4.3 Настройка параметров преобразователя интерфейса Elsys-CU-USB/232-485

При использовании преобразователя интерфейса Elsys-CU-USB/232-485 для обеспечения максимального быстродействия требуется настройка параметров преобразователя в диспетчере устройств Windows.

В узле «Порты (COM и LPT)» дерева устройств следует открыть окно со свойствами порта, использующегося драйвером, перейти на вкладку «Параметры порта» и нажать кнопку «Дополнительно»

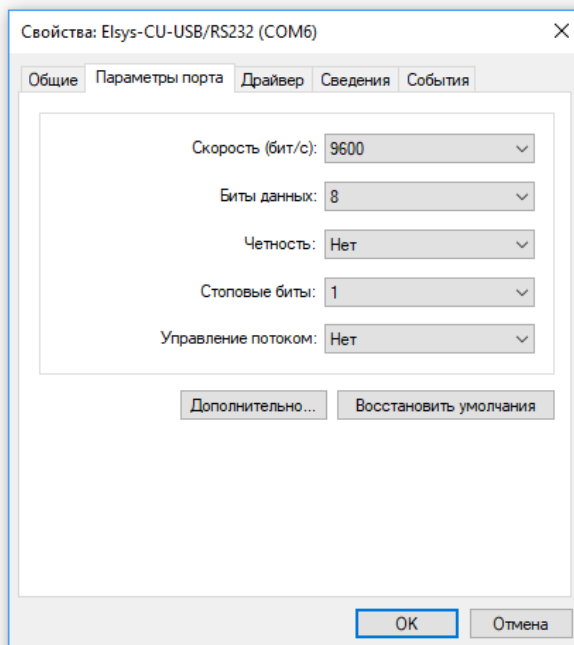


Рисунок 32 – Окно свойств COM-порта

В открывшемся окне следует изменить параметр «Время ожидания», установив значение «1».

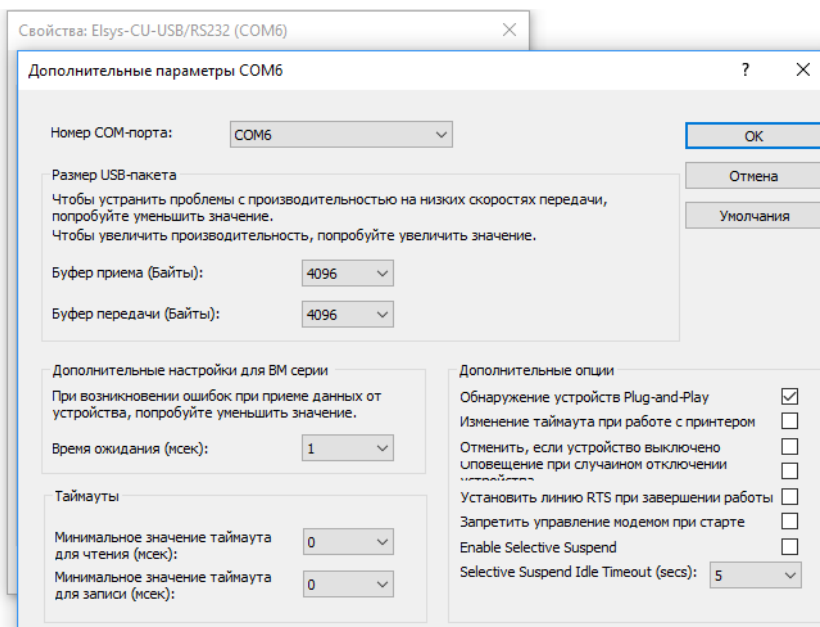


Рисунок 33 – Дополнительные параметры COM-порта Elsys-CU

## 5.5 Настройка контроллеров Elsys-MB

Добавление контроллеров доступа Elsys-MB в базу данных во многих случаях (в особенности, при первом знакомстве с системой) целесообразно выполнять из окна «Поиск оборудования» (функция «Поиск оборудования» описана в п. 4), сразу после обнаружения и начальной настройки подключенного оборудования. Это позволяет



избежать ошибок, связанных с несоответствием характеристики оборудования (адрес, версия, вариант исполнения и т. д.).

Контроллеры также могут быть добавлены в базу данных непосредственно в конфигураторе оборудования, однако в дальнейшем потребуется выполнить поиск, начальную настройку и привести в полное соответствие реальные характеристики оборудования и настройки в базе данных.

Если контроллер доступа подключен через КСК, то для добавления контроллера Elsys-MB в базу данных следует выделить соответствующий узел КСК в дереве устройств и правой кнопкой мыши вызвать контекстное меню, в котором выбрать пункт **«Добавить»**, затем выбрать тип добавляемого контроллера, вставить готовую конфигурацию или загрузить и вставить конфигурацию контроллера из файла (рисунок 34).

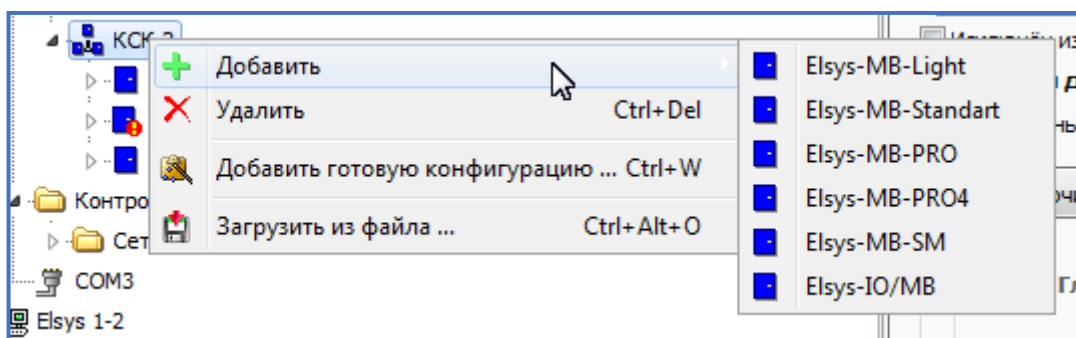


Рисунок 34 – Добавление контроллера Elsys-MB, подключенного через КСК

Если контроллер доступа подключен через COM-порт, то для добавления контроллера Elsys-MB в базу данных следует выделить соответствующий узел COM-порта в дереве устройств, далее действия аналогичны предыдущему случаю (рисунок 35).

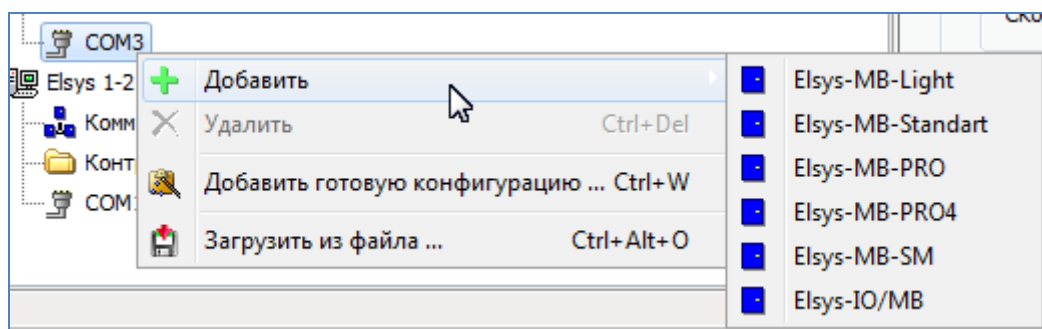


Рисунок 35 – Добавление контроллера Elsys-MB, подключенного через COM-порт

Окно свойств контроллера доступа Elsys-MB содержит четыре вкладки с параметрами (рисунок 36): «Основные», «Дополнительные», «Контроль последовательности прохода» и вкладку «Описание конфигурации», которая содержит текстовое описание конфигурации контроллера, доступное для редактирования.

The screenshot shows the configuration window for the Elsys-MB controller, with the 'Basic' tab selected. The configuration is organized into several sections:

- General Information:** Device name is 'Контроллер 1.1', address is '1', type is 'Elsys-MB-Standard', and version is '2.63'. There is a checkbox for 'Exclude from survey' and a field for 'Access card number size' set to 'As in driver (6 bytes)'.
- Database Format:** Memory expansion module is 'ELSYS-XB32'. There is a checkbox for 'Use PIN codes'. Parameters include 'Number of access cards without time limit' (33718, up to 48040), 'Number of access cards with time limit' (0, up to 7161), and 'Event buffer size' (13040 messages).
- Advanced Settings:** A checked checkbox for 'Expanded configuration options'. Parameters include 'Number of access levels' (3600, up to 32000) and 'Number of time intervals' (1800, up to 12030).
- Options:** Keyboard type is 'Wiegand (shared with reader)'. There are three checked checkboxes: 'Use tamper', 'Use power monitoring', and 'Monitor signal «Battery discharged»'. The reader interface is also 'Wiegand'. A checked checkbox at the bottom states 'Install devices after reset to initial state'.

Рисунок 36 - Основные параметры контроллера Elsys-MB

### 5.5.1 Вкладка «Основные»

«**Наименование устройства**» – наименование устройства, которое можно изменить в целях более удобного представления информации.

«**Подключение через**» – указывает, куда подключен данный контроллер – к COM-порту или к сетевому контроллеру. Для изменения подключения необходимо выбрать в выпадающем списке COM-порт или сетевой контроллер. «Перемещение» контроллера возможно только в пределах одного сервера оборудования. Чтобы подключить контроллер доступа к линии связи другого сервера оборудования следует удалить его из линии связи текущего сервера оборудования и подключить его к линии связи требуемого сервера оборудования, воспользовавшись копированием/вставкой конфигурации или сохранением/загрузкой конфигурации в файл.

«**Адрес**» – уникальный идентификатор контроллера в пределах одной линии связи RS-485. Может принимать значения от 1 до 63. Следует помнить, что изменение адреса в базе данных не вызывает автоматического изменения физического адреса прибора, и наоборот. В каждой линии связи RS-485, подключенной к COM-порту или к сетевому контроллеру, контроллерам Elsys-MB следует присваивать адреса начиная с № 1, в порядке возрастания, без пропусков.

**«Версия»** – соответствует версии встроенного управляющего программного обеспечения контроллера Elsys-MB (версии прошивки). Версия прибора анализируется драйвером при выборе алгоритма инициализации, при формировании управляющих команд и должна соответствовать реальному значению, прочитанному из контроллера.

**Внимание!** Неправильное задание номера версии может вызвать некорректную работу системы с оборудованием.

Список всех известных версий прошивок контроллеров хранится в динамической библиотеке драйвера оборудования Elsys. В свойствах контроллера список версий прошивки (рисунок 37) включает список всех известных версий прошивки и версий прошивок контроллеров Elsys-MB из БД с учетом варианта исполнения контроллера. Несоответствие версии из списка реальному значению отображается цветом фона. На сером фоне отображаются версии, которые меньше реальной версии контроллера, на желтом фоне отображаются версии, которые старше реальной версии контроллера, на красном фоне – номера неизвестных версий прошивки.

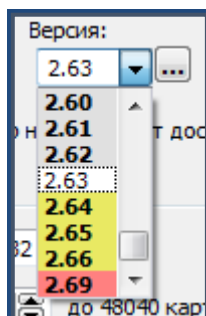


Рисунок 37 – Список версий в свойствах контроллера Elsys-MB

**«Тип (вариант исполнения)»** – вариант исполнения прибора. В текущей версии комплекса поддерживается работа с исполнениями PRO4, PRO, Standard, Light, SM, а также с модулем Elsys-IO/MB.

**«Исключён из опроса»** – при выключении опции контроллер перестаёт опрашиваться драйвером, при выключении опции контроллер начинает опрашиваться драйвером.

**Внимание!** При включении опроса требуется полная инициализация контроллера.

**«Размер номеров карт доступа»** – параметр отображает размер номеров карт доступа в контроллере и не доступен для редактирования. Размер номеров карт в контроллере устанавливается автоматически в соответствии с одноимённой настройкой в свойствах драйвера.

Размер номеров карт 6 байт поддерживается в контроллерах вариантов исполнения «Elsys-MB-Light», «Elsys-MB-Standard», «Elsys-MB-PRO» и «Elsys-MB-PRO4» с версией прошивки 2.63 и выше. Кроме того, если контроллеры доступа подключены через КСК, то требуется версия прошивки КСК 2.10 и выше.

Если размер 6 байт в контроллере не поддерживается, то название параметра отображается в виде гиперссылки красного цвета (рисунок 38), при нажатии на которую выводится сообщение о несоответствии данных (рисунок 39).

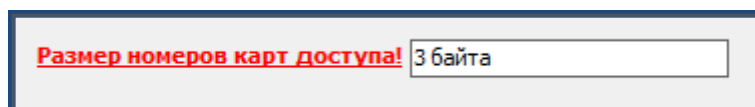


Рисунок 38 – Отображение некорректного значения размера номеров карт в контроллере

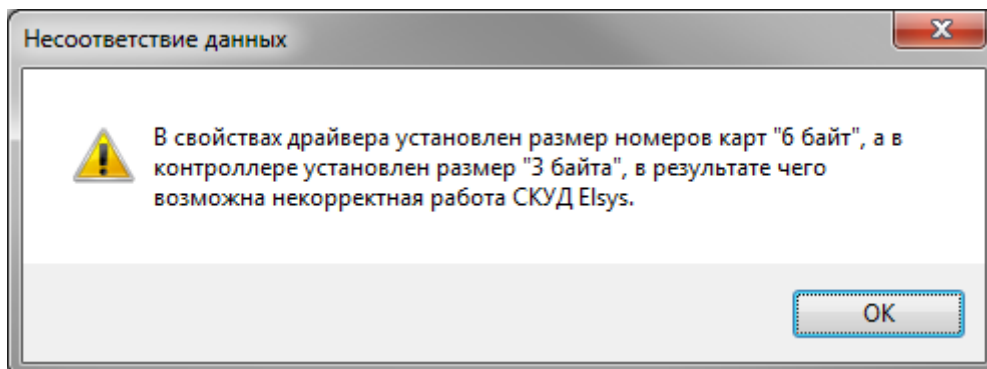



Рисунок 39 – Сообщение о несоответствии размера номеров карт в контроллере

**Внимание!** После изменения размера номера карт в контроллере требуется его полная инициализация.

«Модуль расширения памяти» – опция, определяющая тип или наличие модуля расширения памяти. Возможные значения – «Нет», «Elsys-XB2», «Elsys-XB8», «Elsys-XB32», «Elsys-XB64», «Elsys-XB132».

**Внимание!** Неправильное задание номера версии, типа прибора и типа модуля расширения может вызвать некорректную работу системы.

При несоответствии версии прошивки, варианта исполнения или типа модуля расширения реальным значениям, прочитанным из прибора, а также для новых приборов, добавленных в конфигураторе контроллер отображается значком с восклицательным знаком , а метки соответствующих свойств отображаются в виде гиперссылок красного цвета, с помощью которых можно получить информацию о реальных значениях и, по возможности, установить их корректное значение (рисунок 40).

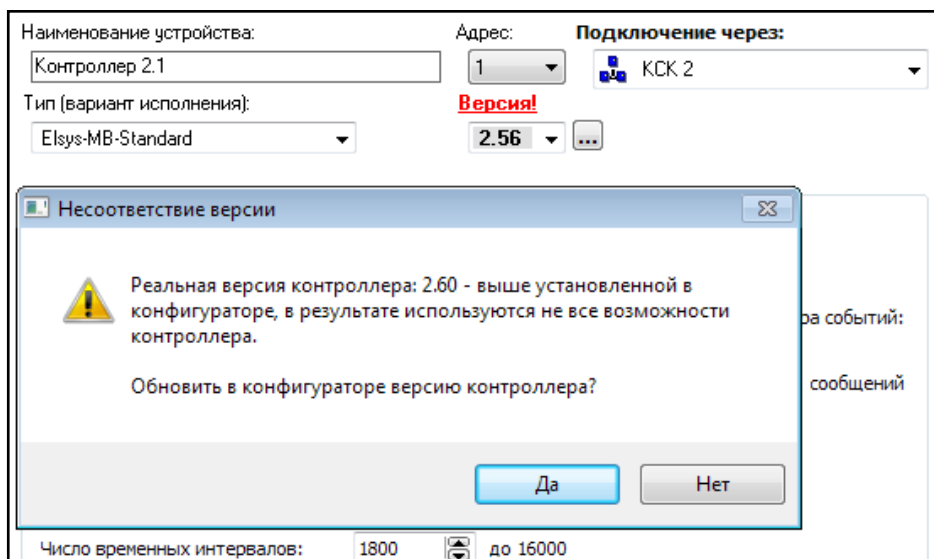


Рисунок 40 – Сообщение о несоответствии версии

Обновление реальных значений версий прошивки, варианта исполнения и типа модуля расширения выполняется автоматически после установления связи с контроллером и после выполнения поиска контроллеров.

**«Тип клавиатур»** – «Матрица 3x4» или «Wiegand совмещённая со считывателем». Клавиатуры разных типов одновременно использоваться не могут. Данные о входах и выходах, используемых для подключения клавиатур, приведены в «Руководстве по эксплуатации СКУД Elsys».

**«Интерфейс считывателей»** – Wiegand или Touch Memory.

**«Использовать PIN-коды»** – эту опцию необходимо включать, если предполагается использование PIN-кодов. При включенном параметре максимальное количество карт уменьшается на 25%.

Группа настроек **«Формат базы данных»** используется для задания распределения памяти контроллера между числом карт, временных интервалов, элементов уровней доступа и числом событий.

**«Число карт доступа без ограничения срока действия»** – определяет максимальное количество постоянных карт в памяти контроллера.

**«Число карт доступа с ограничением срока действия»** – определяет суммарное число временных и разовых карт в памяти контроллера.

**«Расширенные возможности настройки»** – позволяют задавать число элементов уровней доступа и временных блоков, а также вести подсчёт количества персонала.

**«Число элементов уровней доступа»** – определяет максимальное количество элементов уровней доступа. В элемент уровня доступа входит считыватель и назначенный для него временной блок. Описание уровня доступа может занимать в памяти контроллера от одного до четырёх элементов.

**«Число временных интервалов»** – определяет максимальное количество временных интервалов.

***Внимание!** Расширенные возможности настройки доступны для контроллеров имеющих номер версии встроенного ПО 2.53 или старше и установленный модуль расширения памяти.*

**«Использовать тампер»** – если эта опция включена (по умолчанию), то вход 20 используется для подключения извещателя вскрытия корпуса (как правило, это – нормально замкнутый контакт). Если эта опция отключена, вход может использоваться в качестве обычного цифрового входа.

**«Использовать мониторинг питания»** – если эта опция включена (по умолчанию), то вход 21 используется для подключения выхода мониторинга сетевого питания.

**«Мониторинг сигнала «Аккумулятор разряжен»** – если эта опция включена, то вход 15 будет использоваться для мониторинга состояния аккумулятора.

«Устанавливать устройства после сброса в исходное состояние» – если эта опция включена, то после сброса или включения питания контроллера все устройства (входы, выходы, двери, разделы и т. д.) приходят в исходное состояние, а если настройка выключена – состояния всех устройств восстанавливаются.

### 5.5.2 Вкладка «Дополнительные»

Свойства контроллера на вкладке «Дополнительные» показаны на рисунке 41.

Опция «Автоматическая инициализация» позволяет задать алгоритм автоматической инициализации для выбранного контроллера. Соответственно, можно задать инициализацию контроллера в соответствии с настройками драйвера (см. п. 5.1.2), индивидуально, в заданное время, либо не проводить автоматическую инициализацию.

Опция «Завершать ввод PIN-кода символом \* / Завершать ввод PIN-кода символом # (как в N-1000)» определяет, каким символом завершается ввод PIN-кода.

«Тайм-аут для режима MULTIMASTER» (0-255 с) – время ожидания контроллером посылки очередного устройства в режиме MULTIMASTER. Значению 0 соответствуют установки по умолчанию (конкретные значения зависят от скорости обмена).

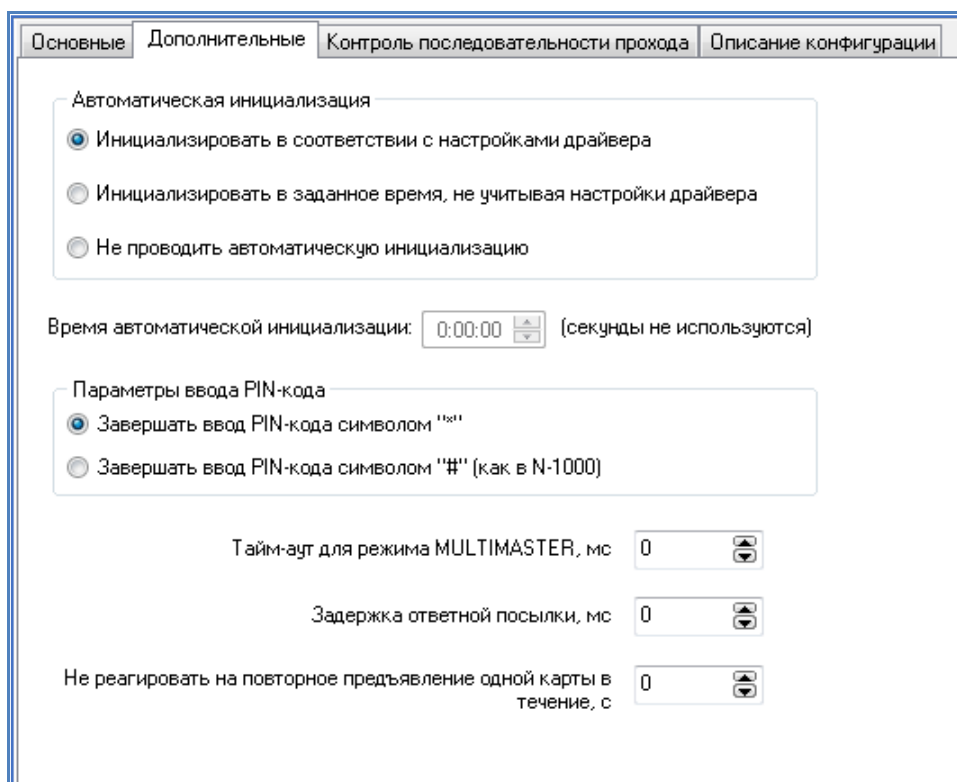


Рисунок 41 –Дополнительные параметры контроллера

«Задержка ответной посылки» (0-255 мс) – эта опция может применяться для адаптации контроллера к условиям, в которых немедленный ответ вызывает потерю данных.

Обе описанные выше опции рекомендуется изменять лишь в тех случаях, когда для удлинения линии связи RS-485 используется устройства, вносящие дополнительные задержки (например, конвертеры «Ethernet-RS-485»).

«Не реагировать на предъявление одной карты в течение ...» – настройка, обеспечивающая отсутствие реакции на повторное предъявление одной карты любому считывателю контроллера в течение заданного времени. Может использоваться при создании различного рода «усиленных» алгоритмов доступа.

### 5.5.3 Вкладка «Контроль последовательности прохода»

Свойства контроллера на вкладке «Контроль последовательности прохода» показаны на рисунке 42.

«Использовать в соответствии с настройками драйвера (сетевого контроллера)» - если выбрана эта опция, то контроллер используется в глобальном контроле последовательности прохода, обмениваясь информацией об изменении пользователями зон доступа.

«Использовать локальный контроль последовательности прохода» – при включенной опции контроллер будет осуществлять контроль последовательности прохода через обслуживаемую им дверь (или турникет). Опция имеет смысл только в сочетании с двусторонней точкой доступа.

Основные | Дополнительные | **Контроль последовательности прохода** | Описание конфигурации

Настройка контроля последовательности прохода

Использовать в соответствии с настройками сетевого контроллера

Использовать локальный контроль последовательности прохода

Не использовать

Сброс в полночь

Временной контроль последовательности прохода

Использовать временной контроль последовательности прохода

Интервал через который сбрасывается информация о прошедшей карте, мин.:

Контроллер используется в следующих областях контроля:

Вне территории (Дверь 5)  
Вне территории (Дверь 6)  
На территории (Дверь 5)  
На территории (Дверь 6)

Рисунок 42 - Настройки контроля последовательности прохода

«Не использовать» – контроллер не используется для контроля последовательности прохода.



«Сброс в полночь» – если эта опция включена, то в 0 час 0 мин в контроллере ежедневно очищается информация о текущей зоне доступа всех пользователей.

Группа настроек «**Временной контроль последовательности прохода**» позволяет включить временной контроль последовательности прохода, когда информация о прошедшей карте сбрасывается через заданный промежуток времени.

Опция «**Использовать временной контроль последовательности прохода**» позволяет включить временной контроль последовательности прохода.

«**Интервал через который сбрасывается информация о прошедшей карте, мин**» – определяет интервал времени в минутах, через который сбрасывается информация о прошедшей карте.

**Внимание!** Режим временного контроля последовательности прохода доступен для контроллеров имеющих номер версии встроенного ПО 2.53 или старше и установленный модуль расширения памяти. Кроме того, для работы этого режима должна быть включена опция «**Расширенные возможности настройки**» и выключена опция «**Вести подсчёт количества персонала в областях контроля**» в свойствах дверей (турникетов, ворот) (рисунок 43).

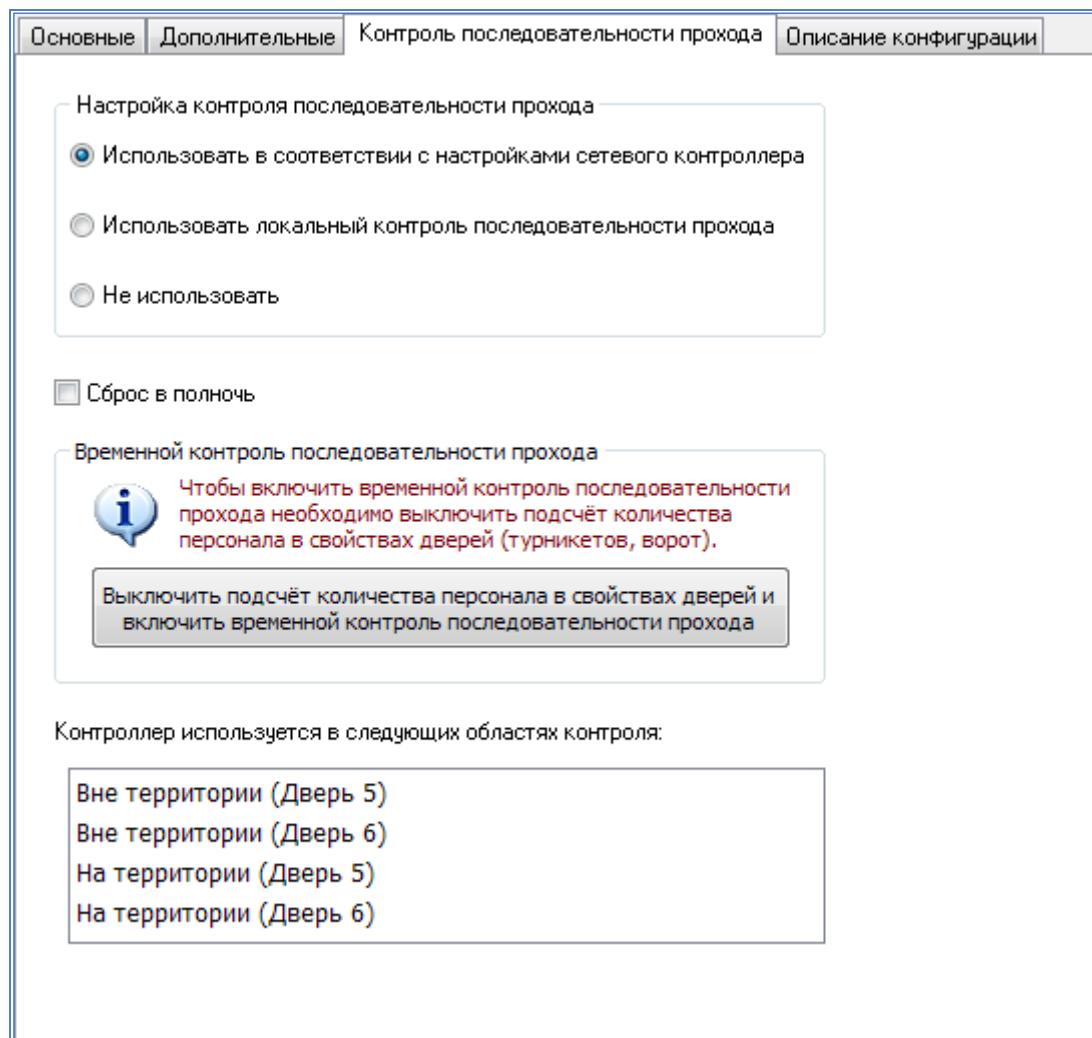


Рисунок 43 – Настройки контроля последовательности прохода при включенном подсчёте количества персонала в свойствах дверей



Список **«Контроллер используется в следующих областях контроля»** – показывает названия всех областей контроля, в которые входят двери данного контроллера.

## 5.6 Настройка контроллеров Elsys-MB-IP

Добавление контроллеров доступа Elsys-MB-IP в базу данных во многих случаях (в особенности, при первом знакомстве с системой) целесообразно выполнять из окна «Поиск оборудования» (функция «Поиск оборудования» описана в п. 3), сразу после обнаружения и начальной настройки подключенного оборудования. Это позволяет избежать ошибок, связанных с несоответствием характеристики оборудования (адрес, версия, вариант исполнения и т. д.).

Контроллеры также могут быть добавлены в базу данных непосредственно в конфигураторе оборудования, однако в дальнейшем потребуется выполнить поиск, начальную настройку и привести в полное соответствие реальные характеристики оборудования и настройки в базе данных.

Для добавления контроллера Elsys-MB-IP в базу данных в дереве конфигурации следует выделить сетевую группу, в которую входит контроллер и правой кнопкой мыши вызвать контекстное меню, в котором выбрать пункт **«Добавить»**, затем выбрать тип добавляемого контроллера, вставить готовую конфигурацию или загрузить и вставить конфигурацию контроллера из файла (рисунок 44).

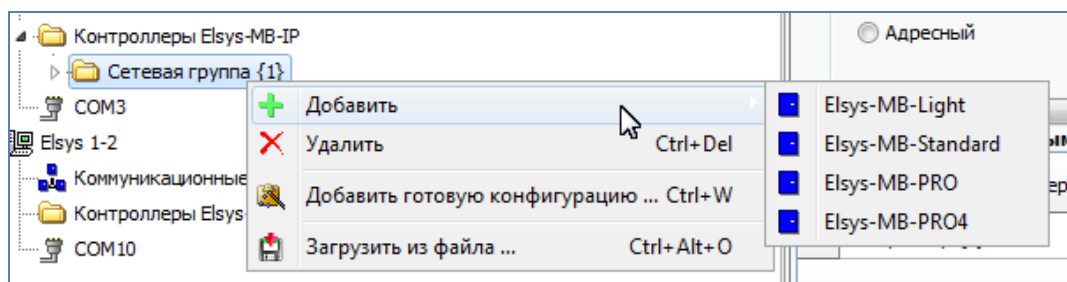


Рисунок 44 – Добавление контроллера Elsys-MB-IP

Если требуемая сетевая группа отсутствует, то сначала следует создать сетевую группу (см. п. 5.3).

Настройка контроллеров Elsys-MB-IP полностью совпадает с настройкой контроллеров Elsys-MB, за исключением способа их подключения, это опции: **«Подключение через:»**, **«Версия Elsys-IP»** и **«Настройки для локальной сети»**(рисунок 45).

**«Подключение через»** – настройка в контроллерах доступа Elsys-MB-IP отображает принадлежность контроллера к сетевой группе. Для изменения сетевой группы необходимо выбрать в выпадающем списке требуемую сетевую группу. «Перемещение» контроллера из одной сетевой группы в другую возможно только в пределах одного сервера оборудования. Для включения контроллера Elsys-MB-IP в сетевую группу другого сервера оборудования, следует удалить контроллер из сетевой группы текущего сервера и добавить его в сетевую группу требуемого сервера оборудования, воспользовавшись копированием/вставкой конфигурации или сохранением/загрузкой конфигурации в файл.

«Версия Elsys-IP» - версия встроенного программного обеспечения (версия прошивки) интерфейсного Ethernet-модуля, который входит в состав контроллеров Elsys-MB-IP.

«Настройки для локальной сети» - используются для подключения контроллеров Elsys-MB-IP к локальной вычислительной сети (ЛВС).

The screenshot displays the configuration interface for an Elsys-MB-IP controller, organized into several sections:

- Basic Information:** Device name is "Контроллер {1}.1" and address is "1".
- Hardware and Software:** Type is "Elsys-MB-PRO", Elsys-MB version is "2.64", and Elsys-IP version is "2.02".
- Access Control:** "Исключён из опроса" is unchecked. Access card size is "Как в драйвере (6 байт)".
- Database Format:** Memory expansion module is "ELSYS-XB64". "Использовать PIN-коды" is unchecked.
- Access Limits:** "Число карт доступа без ограничения срока действия" is 48917 (range 0-97811). "Число карт доступа с ограничением срока действия" is 0 (range 0-24447). "Размер буфера событий" is 44469 messages.
- Advanced Settings:** "Расширенные возможности настройки" is checked. "Число элементов уровней доступа" is 3600 (range 0-65000). "Число временных интервалов" is 1800 (range 0-32000).
- Options:** "Тип клавиатур" is "Wiegand (совмещённая со считывателем)". "Интерфейс считывателей" is "Wiegand". "Использовать тампер", "Использовать мониторинг питания", and "Мониторинг сигнала «Аккумулятор разряжен»" are all checked.
- Reset and Local Network:** "Устанавливать устройства после сброса в исходное состояние" is checked. The "Настройки для локальной сети" section includes:
  - IP Address: 192.168.21.156
  - Subnet Mask: 255.255.255.0
  - Gateway: 0.0.0.0

Рисунок 45 – Свойства контроллера Elsys-MB-IP

«IP-адрес» - IP-адрес контроллера Elsys-MB-IP в ЛВС.

«Маска подсети» - маска подсети для контроллера Elsys-MB-IP .

«Шлюз» - IP-адрес шлюза в ЛВС.

## 5.7 Работа с конфигурациями контроллеров Elsys-MB и Elsys-MB-IP

В конфигураторе оборудования имеется возможность копировать, сохранять в файл, загружать из файла или вставлять скопированные конфигурации контроллеров доступа Elsys-MB и Elsys-MB-IP. Конфигурация контроллера содержит все настройки оборудования, входящего в его состав (точки доступа, считыватели, входы и выходы, взаимодействия).

Если конфигурация вставляется или загружается в узел сетевого контроллера, сетевой группы или COM-порта, то она будет **добавлена** как новая.

Если конфигурация вставляется или загружается в узел выбранного контроллера доступа, то она **заменит** существующую конфигурацию.

***Внимание!** После вставки или замены конфигураций контроллеров необходимо проверить, и, если нужно, установить заново версию, вариант исполнения контроллера, тип модуля расширения памяти.*

### 5.7.1 Использование готовых конфигураций

В комплекте с ПО «Бастион-2» поставляются конфигурации контроллеров, представляющие собой готовые решения для большинства типовых задач (одно- и двусторонний контроль доступа с электромагнитными и электромеханическими замками, турникет, шлагбаум, шлюз и т. д.). Файлы готовых конфигураций поставляются на дистрибутивном диске. При установке комплекса «Бастион-2» они помещаются в каталог «...\Bastion\ElsConfigs». С готовыми конфигурациями настоятельно рекомендуется ознакомиться – это в значительной мере облегчит дальнейшую настройку системы.

Для вставки готовой конфигурации необходимо выбрать узел КСК, сетевой группы или COM-порта, в зависимости от требуемого подключения и вызвать контекстное меню, в котором выбрать пункт **«Добавить готовую конфигурацию»** (рисунок 46).

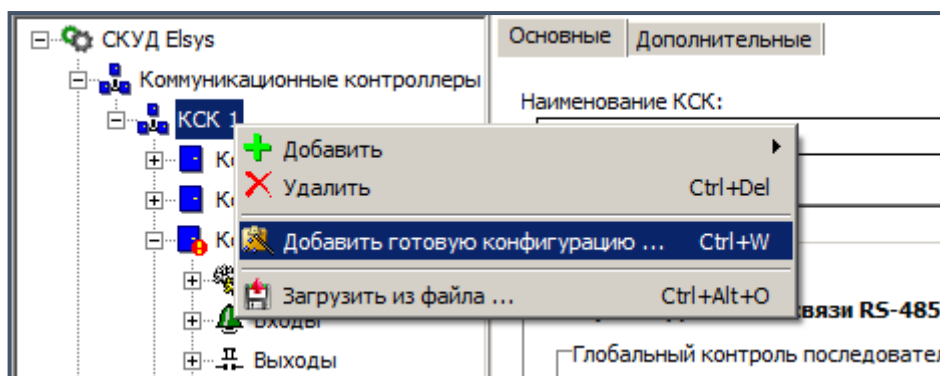


Рисунок 46 – Добавление подключенного к КСК контроллера Elsys-MB с готовой конфигурацией

В открывшемся окне (рисунок 47) следует указать вариант исполнения контроллера и версию прошивки, после чего можно выбрать необходимую конфигурацию из готовых и ранее сохраненных конфигураций (сохраненные конфигурации будут видны в данном окне, только если они были сохранены в папке «...\Bastion\ElsConfigs»).

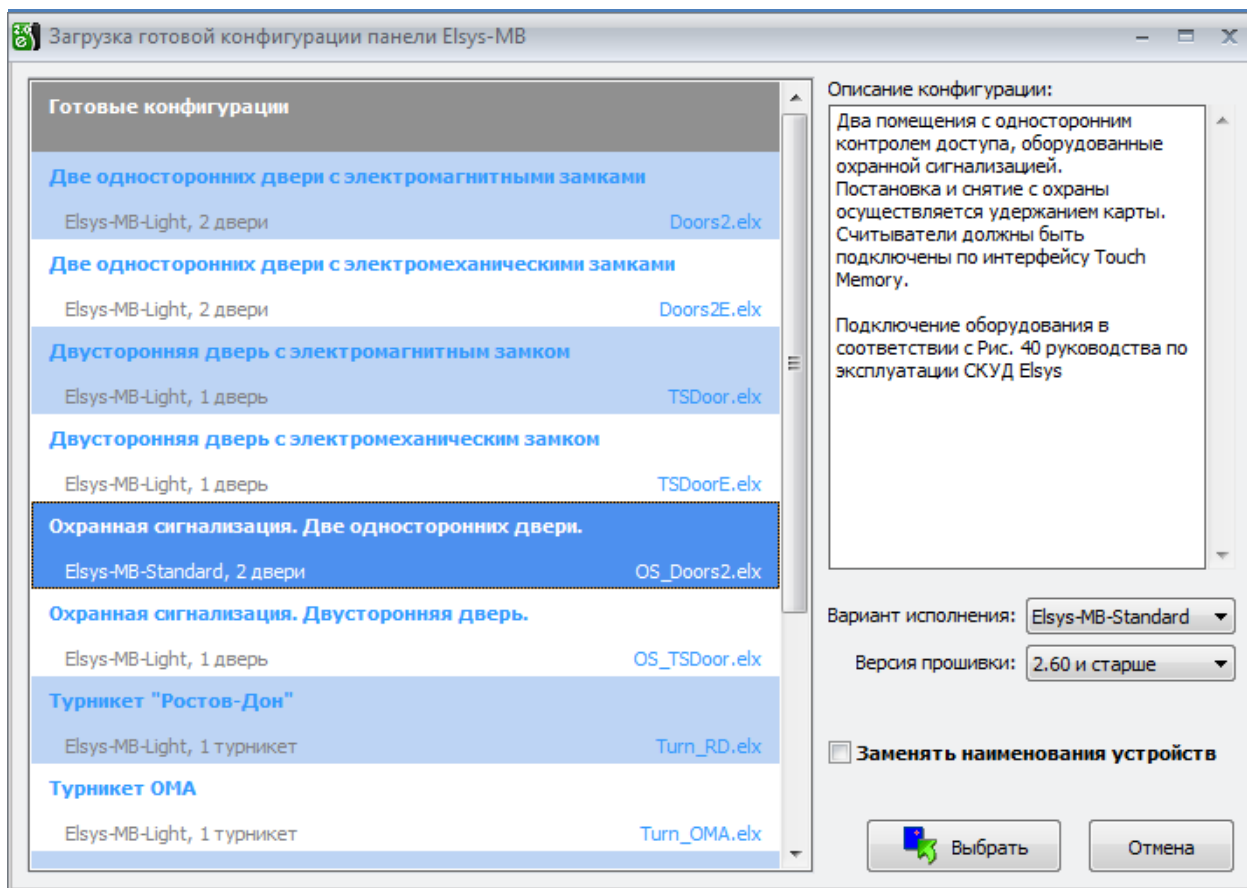


Рисунок 47 – Окно выбора конфигурации при добавлении готовой конфигурации

Опция **«Заменять наименования устройств»** позволяет заменить стандартные названия устройств на заданные в конфигурации.

После того как конфигурация выбрана, нажмите **«Выбрать»** для вставки конфигурации в дерево устройств.

Чтобы заменить конфигурацию уже добавленного контроллера, следует из его контекстного меню в дереве конфигурации выбрать команду **«Заменить готовой конфигурацией»** (рисунок 48). При замене конфигурации в окне выбора готовых конфигураций опции **«Вариант исполнения»** и **«Версия прошивки»** соответствуют свойствам контроллера в конфигураторе и не доступны для редактирования (рисунок 49).

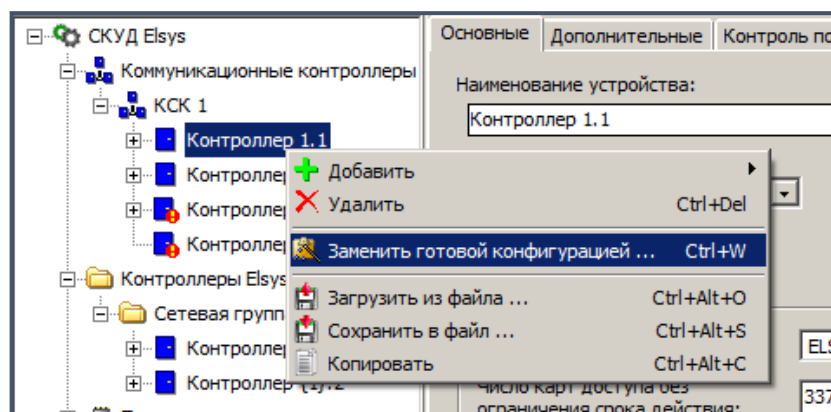


Рисунок 48 – Замена конфигурации контроллера Elsys-MB, подключенного к КСК

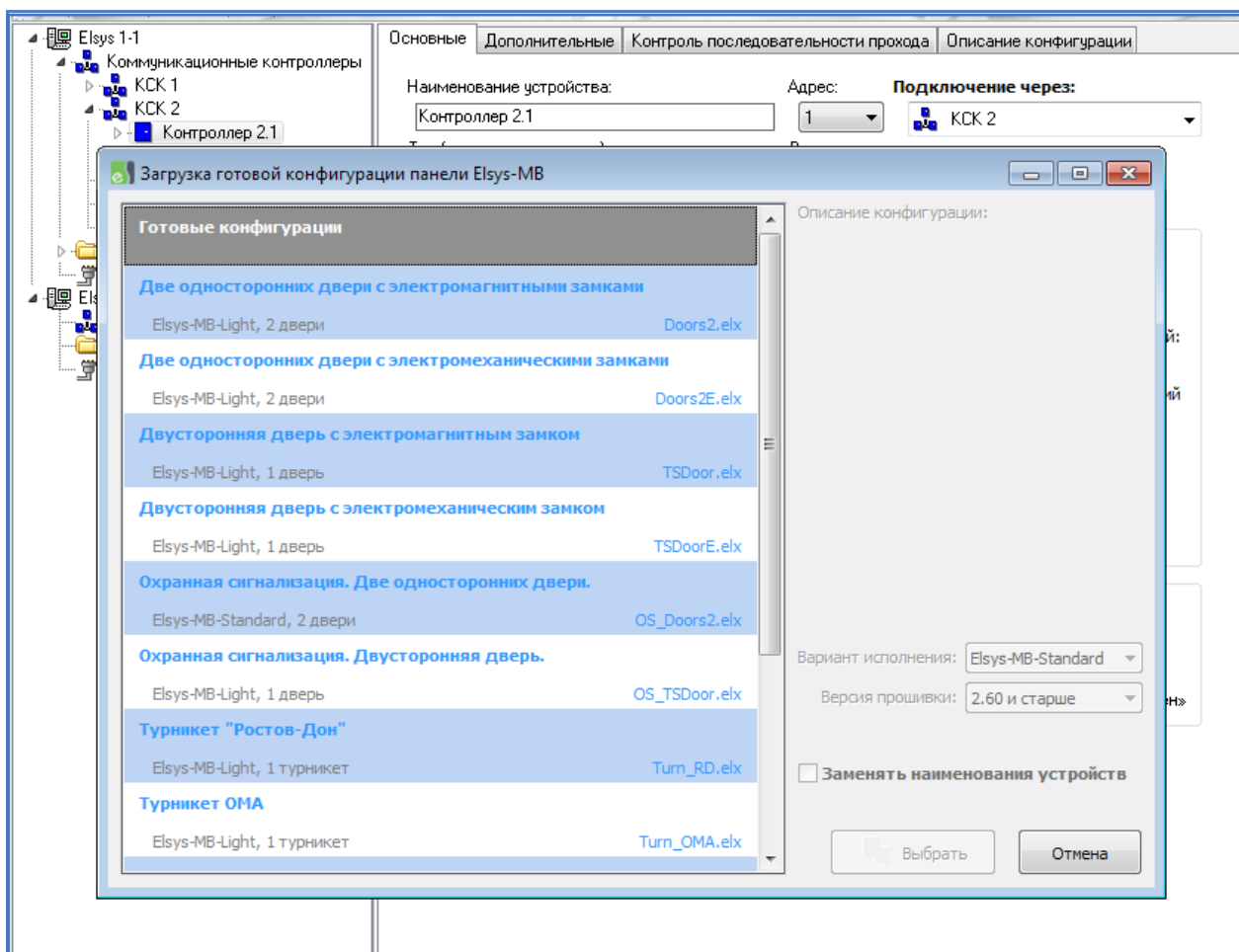


Рисунок 49 – Замена конфигурации контроллера

В появившемся окне следует выбрать необходимую конфигурацию и нажать кнопку **«Выбрать»**.

В таблице 4 приведён перечень готовых конфигураций, поставляемых на дистрибутивном диске, и их краткое описание.

Большинство конфигураций созданы на основе типовых схем подключения оборудования, приведённых в документах «Руководство по эксплуатации СКУД Elsys» и «Руководство по эксплуатации Elsys-MB-SM».

Таблица 4 - Перечень готовых конфигураций

№	Имя файла с расширением «.elx»	Для вариантов исполнения					Схема подключений краткое описание конфигурации
		Light	Standard	PRO	PRO4	SM	
1	TSDoorE	+	+	+	-	-	Схема подключений Рисунок 21 РЭ СКУД Elsys

Таблица 4 - Перечень готовых конфигураций

№	Имя файла с расширением «.elx»	Для вариантов исполнения					Схема подключений краткое описание конфигурации
		Light	Standard	PRO	PRO4	SM	
							<b>Описание конфигурации</b> Двусторонняя дверь с электромеханическим замком
2	Doors2E	+	+	+	-	-	<b>Схема подключений</b> Рисунок 22 РЭ СКУД Elsys <b>Описание конфигурации</b> Две односторонних двери с электромеханическими замками
3	PRO4Doors2E	-	-	-	+	-	<b>Схема подключений</b> Рисунок 23 РЭ СКУД Elsys <b>Описание конфигурации</b> Две двусторонних двери с электромеханическими замками
4	PRO4Doors4E	-	-	-	+	-	<b>Схема подключений</b> Рисунок 24 РЭ СКУД Elsys <b>Описание конфигурации</b> Четыре односторонних двери с электромеханическими замками
5	TSDoor	+	+	+	-	-	<b>Схема подключений</b> Рисунок 25 РЭ СКУД Elsys <b>Описание конфигурации</b> Двусторонняя дверь с электромагнитным замком
6	Doors2	+	+	+	-	-	<b>Схема подключений</b> Рисунок 26 РЭ СКУД Elsys

Таблица 4 - Перечень готовых конфигураций

№	Имя файла с расширением «.elx»	Для вариантов исполнения					Схема подключений краткое описание конфигурации
		Light	Standard	PRO	PRO4	SM	
							<b>Описание конфигурации</b> Две односторонних двери с электромагнитными замками
7	PRO4Doors2	-	-	-	+	-	<b>Схема подключений</b> Рисунок 27 РЭ СКУД Elsys
							<b>Описание конфигурации</b> Две двусторонних двери с электромагнитными замками
							<b>Схема подключений</b> Рисунок 28 РЭ СКУД Elsys
							<b>Описание конфигурации</b> Четыре односторонних двери с электромагнитными замками
8	PRO4Doors4	-	-	-	+	-	<b>Схема подключений</b> Рисунок 29 РЭ СКУД Elsys
							<b>Описание конфигурации</b> Шлюз, состоящий из двух дверей с электромагнитными замками
							<b>Схема подключений</b> Рисунок 30, рисунок 31, рисунок 32 РЭ СКУД Elsys
							<b>Описание конфигурации</b> Турникеты PERCo моделей PERCo-TTR-04.1, PERCo-RTD-03s, PERCo-TTR-04W-24
9	GatewayA	+	+	+	-	-	<b>Схема подключений</b> Рисунок 30, рисунок 31, рисунок 32 РЭ СКУД Elsys
							<b>Описание конфигурации</b> Турникеты PERCo моделей PERCo-TTR-04.1, PERCo-RTD-03s, PERCo-TTR-04W-24
							<b>Схема подключений</b> Рисунок 29 РЭ СКУД Elsys
							<b>Описание конфигурации</b> Шлюз, состоящий из двух дверей с электромагнитными замками
10	Turn_PERCo1	-	+	+	-	-	<b>Схема подключений</b> Рисунок 29 РЭ СКУД Elsys
							<b>Описание конфигурации</b> Шлюз, состоящий из двух дверей с электромагнитными замками
							<b>Схема подключений</b> Рисунок 30, рисунок 31, рисунок 32 РЭ СКУД Elsys
							<b>Описание конфигурации</b> Турникеты PERCo моделей PERCo-TTR-04.1, PERCo-RTD-03s, PERCo-TTR-04W-24

Таблица 4 - Перечень готовых конфигураций

№	Имя файла с расширением «.elx»	Для вариантов исполнения					Схема подключений краткое описание конфигурации
		Light	Standard	PRO	PRO4	SM	
							Конфигурация предназначена для всех моделей турникетов, выпускаемых компанией PERCo.  Для мониторинга каждого направления прохода используется отдельный датчик.
11	Turn_PERCo2	-	+	+	-	-	<b>Схема подключений</b>
							Рисунок 32 РЭ СКУД Elsys
							<b>Описание конфигурации</b>
							Конфигурация предназначена для некоторых моделей турникетов компании PERCo (например, PERCo-TTR-04W-24), использующих режим, при котором в процессе прохода последовательно срабатывают  два датчика прохода (последовательность срабатывания зависит от направления прохода).  К контроллеру Elsys-MB необходимо подключать только один из них!
12	Turn_RD	+	+	+	-	-	<b>Схема подключений</b>
							Рисунок 33 РЭ СКУД Elsys
							<b>Описание конфигурации</b>
							Конфигурация для турникетов и калиток "Ростов-Дон"
13	Turn_OMA	+	+	+	-	-	<b>Схема подключений</b>
							Рисунок 34 РЭ СКУД Elsys
							<b>Описание конфигурации</b>



Таблица 4 - Перечень готовых конфигураций

№	Имя файла с расширением «.elx»	Для вариантов исполнения					Схема подключений краткое описание конфигурации
		Light	Standard	PRO	PRO4	SM	
							Конфигурация для турникета ОМА с блоком управления DD.958
14	PRO4Turns2	-	-	-	+	-	<b>Схема подключений</b>
							Рисунок 35 РЭ СКУД Elsys
							<b>Описание конфигурации</b>
							Конфигурация для двух турникетов PERCo, имеющих по два датчика прохода
15	PW500	-	-	-	+	-	<b>Схема подключений</b>
							Рисунок 36 РЭ СКУД Elsys
							<b>Описание конфигурации</b>
							Конфигурация, предназначенная для совместного использования турникета PERCo и картосборника PW-500, используемого для сбора разовых карт на выходе из предприятия.  Для разовых карт необходимо в профилях настроек персонала  СКУД Elsys включить опцию "Действие 1".
16	Shlb1	-	+	+	-	-	<b>Схема подключений</b>
							Рисунок 37 РЭ СКУД Elsys
							<b>Описание конфигурации</b>

Таблица 4 - Перечень готовых конфигураций

№	Имя файла с расширением «.elx»	Для вариантов исполнения					Схема подключений краткое описание конфигурации
		Light	Standard	PRO	PRO4	SM	
							Базовая конфигурация, обеспечивающая работу с большинством моделей шлагбаумов и приводов ворот. Разрабатывалась для работы со шлагбаумом CAME, имеющим блок управления ZL-37. Если датчик открытого состояния отсутствует, необходимо соединить с цепью GND вход, предназначенный для его подключения, или исключить его из конфигурации шлагбаума, выбрав «Нет» в поле «Датчик открытого состояния». Если отсутствует датчик закрытого состояния, необходимо соединить с цепью GND вход, предназначенный для его подключения, или исключить его из конфигурации шлагбаума, выбрав «Нет» в поле «Датчик закрытого состояния», и, кроме того, в конфигурации в свойствах шлагбаума снять опцию «Отслеживать фактический проход».
17	Shlb_CAME	-	-	+	-	-	<p><b>Схема подключений</b></p> Рисунок 38 РЭ СКУД Elsys
							<p><b>Описание конфигурации</b></p> Конфигурация для работы со шлагбаумом CAME, имеющим блок управления ZL-37. Главные отличительные особенности: - функции безопасного закрывания и автозакрывания реализованы средствами логики контроллера; - в конфигурации имеются датчики присутствия автомобиля.
18	SMDdoors2E	-	-	-	-	+	<p><b>Схема подключений</b></p> Рисунок 7 РЭ Elsys-MB-SM
							<p><b>Описание конфигурации</b></p>

Таблица 4 - Перечень готовых конфигураций

№	Имя файла с расширением «.elx»	Для вариантов исполнения					Схема подключений краткое описание конфигурации
		Light	Standard	PRO	PRO4	SM	
							Две односторонних двери с электромеханическими замками
19	SMTSDoorE	-	-	-	-	+	<b>Схема подключений</b>
							Рисунок 8 РЭ Elsys-MB-SM
							<b>Описание конфигурации</b>
							Двусторонняя дверь с электромеханическим замком
20	SMDdoors2	-	-	-	-	+	<b>Схема подключений</b>
							Рисунок 9 РЭ Elsys-MB-SM
							<b>Описание конфигурации</b>
							Две односторонних двери с электромагнитными замками
21	SMTSDoor	-	-	-	-	+	<b>Схема подключений</b>
							Рисунок 10 РЭ Elsys-MB-SM
							<b>Описание конфигурации</b>
							Двусторонняя дверь с электромагнитным замком
22	OS_TSDoor						<b>Схема подключений</b>
							Рисунок 39 РЭ СКУД Elsys
							<b>Описание конфигурации</b>
							Двусторонняя дверь. Охранная сигнализация.  Помещение с двусторонним контролем доступа, оборудованное охранной сигнализацией. Постановка на охрану осуществляется изнутри помещения с помощью кнопки и карты.
23	OS_Doors2						<b>Схема подключений</b>
							Рисунок 40 РЭ СКУД Elsys

Таблица 4 - Перечень готовых конфигураций

№	Имя файла с расширением «.elx»	Для вариантов исполнения					Схема подключений краткое описание конфигурации
		Light	Standard	PRO	PRO4	SM	
							<p><b>Описание конфигурации</b></p> <p>Две односторонних двери. Охранная сигнализация.</p> <p>Два помещения с односторонним контролем доступа, оборудованные охранной сигнализацией. Постановка и снятие с охраны осуществляется удержанием карты. Считыватели должны быть подключены по интерфейсу Touch Memory.</p>
24	os_PRO4Doors2						<p><b>Схема подключений</b></p> <p>Рисунок 41 РЭ СКУД Elsys</p> <p><b>Описание конфигурации</b></p> <p>Две двусторонних двери. Охранная сигнализация.</p> <p>Два помещения с двусторонним контролем доступа, оборудованные охранной сигнализацией. Постановка на охрану осуществляется изнутри помещения с помощью кнопки и карты.</p>
25	GatewayPro4	-	-	-	+	-	<p><b>Схема подключений</b></p> <p>Схема и подробное иписание находятся в отдельном документе: "Бастион-2 - Elsys. Готовая конфигурация - Шлюз на PRO4.docx"</p> <p><b>Описание конфигурации</b></p> <p>Elsys-MB-Pro4, две 2-сторонних двери. Двери шлюза открываются по очереди, одновременно обе двери открыты быть не могут.</p>
26	TSDoor_Count						<p><b>Схема подключений</b></p> <p>Подключение оборудования в соответствии с Рис. 25 руководства по эксплуатации СКУД Elsys.</p> <p><b>Описание конфигурации</b></p>

Таблица 4 - Перечень готовых конфигураций

№	Имя файла с расширением «.elx»	Для вариантов исполнения					Схема подключений краткое описание конфигурации
		Light	Standard	PRO	PRO4	SM	
							<p>Когда в помещении находится хотя бы один штатный сотрудник, то посетитель может войти в это помещение по выданной ему карте доступа. Если в помещении штатных сотрудников нет – вход посетителей по картам невозможен.</p> <p>Подробное описание приведено в отдельном документе: Бастион-2 - Elsys. Готовая конфигурация - Дверь с подсчетом персонала.docx</p>
27	Door2_unlock						<p><b>Схема подключений</b></p> <p>Подключение оборудования в соответствии с Рис. 26 руководства по эксплуатации СКУД Elsys.</p> <p><b>Описание конфигурации</b></p> <p>При предъявлении служебной карты к входному считывателю меняется состояние двери. Если дверь была в нормальном режиме (доступ по картам), то она переходит в разблокированное состояние (свободный доступ). Если дверь была в разблокированном состоянии – она переходит в нормальный режим.</p> <p>Подробное описание приведено в отдельном документе: "Бастион-2 - Elsys. Готовая конфигурация - Дверь с разблокировкой по служебной карте.docx"</p>

### 5.7.2 Копирование и вставка конфигурации

Для копирования конфигурации контроллера необходимо выбрать контроллер в дереве конфигурации, содержащий конфигурацию, которая будет скопирована, и вызвать контекстное меню, в котором выбрать пункт **«Копировать»** (рисунок 50).

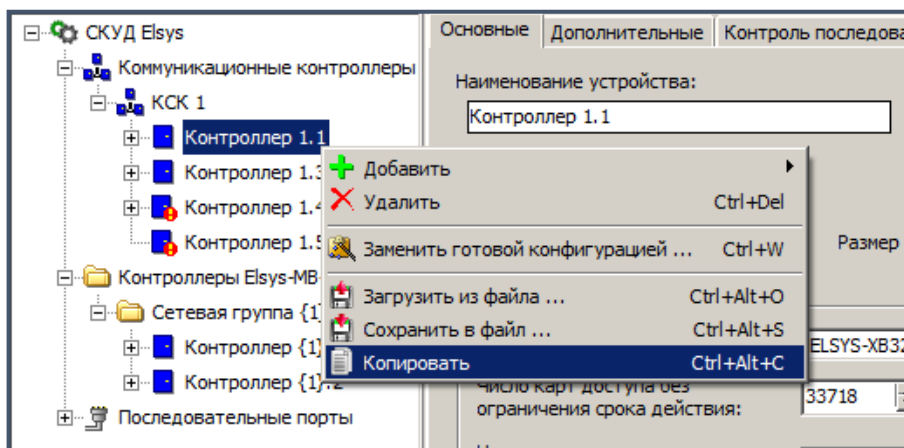


Рисунок 50 - Контекстное меню копирования конфигурации

Скопированную конфигурацию можно добавить из контекстного меню КСК, сетевой группы или СОМ-порта (рисунок 51).

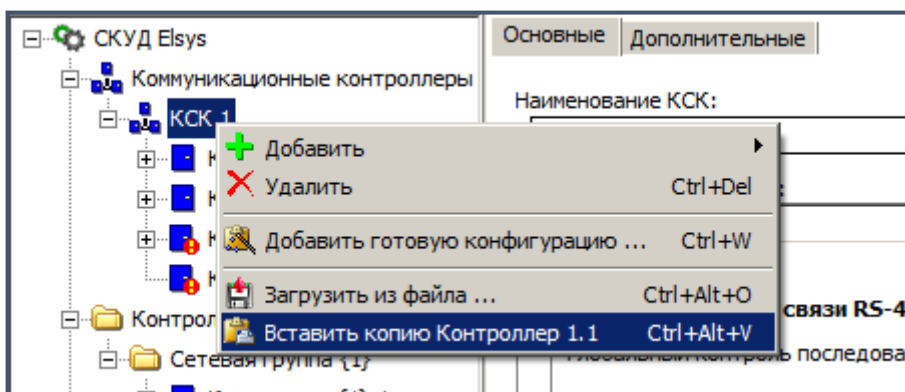


Рисунок 51 – Добавление копии конфигурации

Скопированную конфигурацию можно также вставить в существующий контроллер, используя контекстное меню контроллера, в котором следует заменить конфигурацию (рисунок 52).

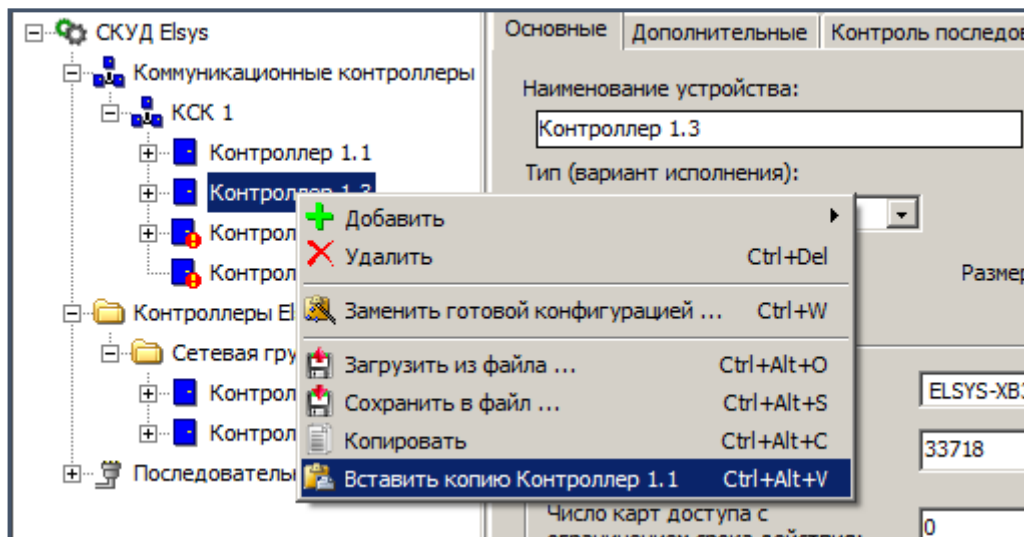


Рисунок 52 – Вставка копии конфигурации в выбранный контроллер

Если скопированная конфигурация и текущая конфигурация панели совпадают по числу и типу дверей и считывателей, то появляется окно (рисунок 53) с запросом на обновление параметров текущей конфигурации на параметры из скопированной конфигурации.

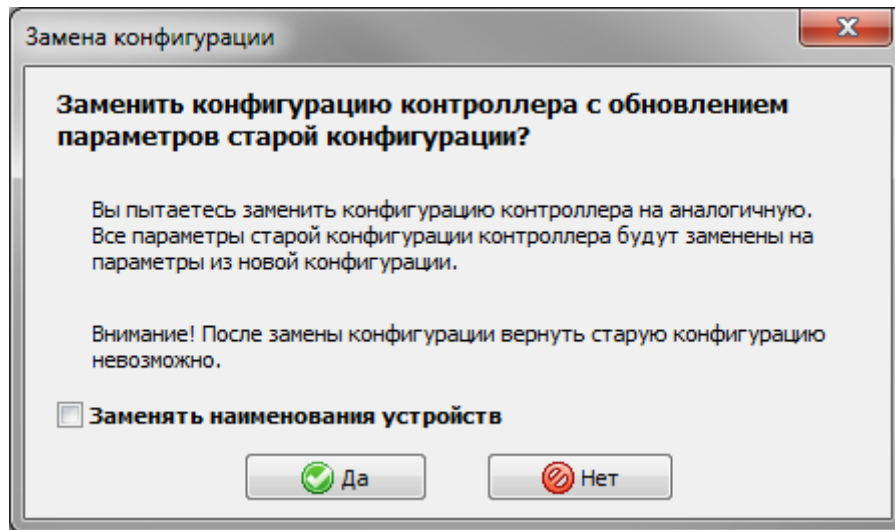


Рисунок 53 - Предупреждение при вставке с заменой параметров

Опция «**Заменять наименования устройств**» позволяет заменить стандартные названия устройств на заданные в конфигурации.

Если скопированная конфигурация и текущая конфигурация панели **НЕ** совпадают по числу и типу дверей и считывателей, то появляется окно с запросом на полное удаление старой конфигурации (рисунок 54).

***Внимание!** В этом случае возможно удаление считывателей из уровней доступа. После вставки конфигурации необходимо проверить уровни доступа на предмет добавления в новых считывателей.*

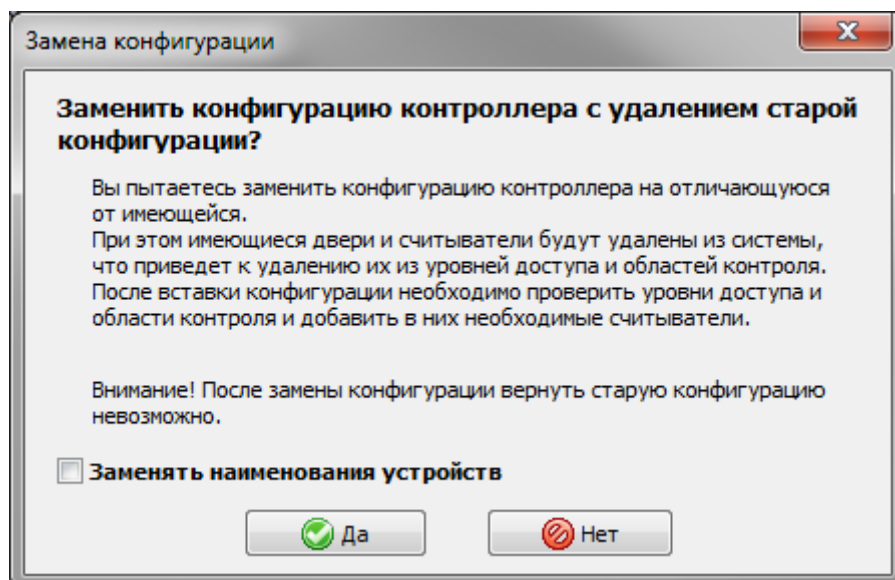


Рисунок 54 - Предупреждение при вставке с удалением старой конфигурации

### 5.7.3 Сохранение и загрузка конфигурации

Для сохранения конфигурации необходимо выбрать узел «Панель», содержащий конфигурацию, которую необходимо сохранить, и вызвать контекстное меню, в котором выбрать пункт «Сохранить в файл» (рисунок 55).

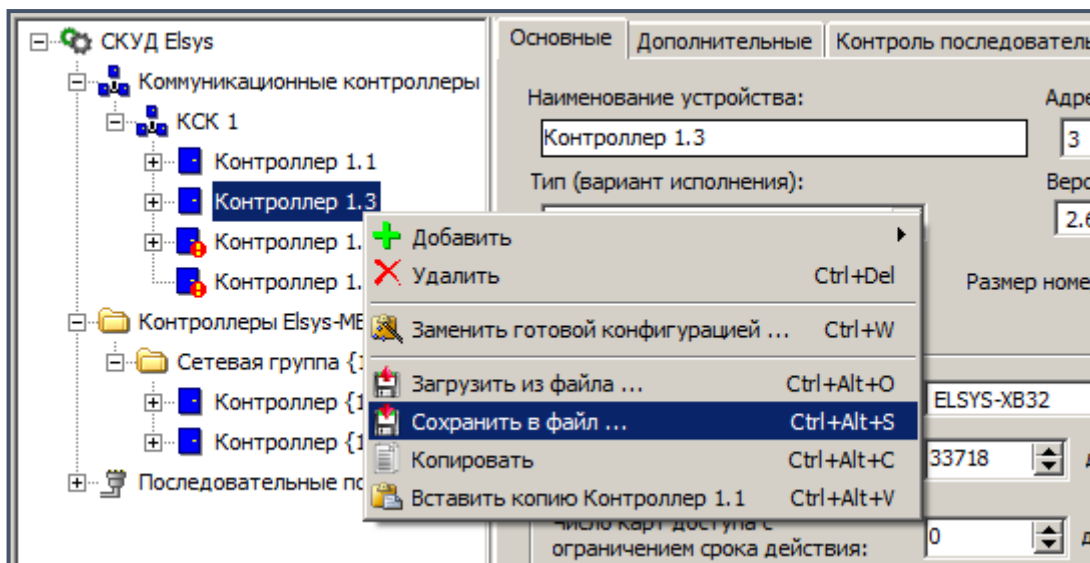


Рисунок 55 - Контекстное меню сохранения конфигурации

В появившемся окне (рисунок 56) необходимо выбрать имя файла и каталог, в который будет сохранена конфигурация.

По умолчанию конфигурации сохраняются в файлах с расширением «.elx» в формате **«Конфигурация контроллера версии 2.60 и выше»**. Формат **«Конфигурация контроллера версии ниже 2.60»** используется для совместимости с предыдущими версиями драйвера «Бастион-2 – Elsys», в которых отсутствует поддержка охранных функций. Конфигурации могут быть также сохранены в старом формате (расширение файла «.els»), использовавшемся в предыдущих (1.5 и ниже) версиях ПО «Бастион-2».



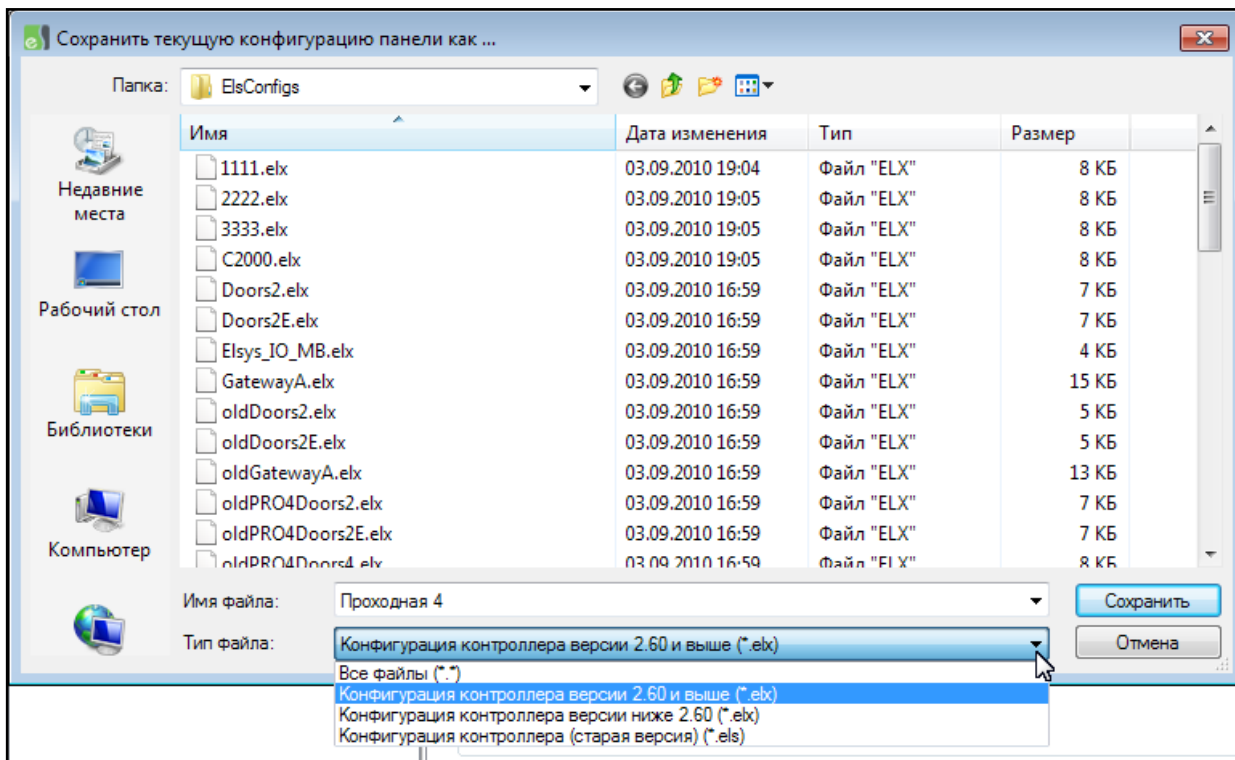


Рисунок 56 - Окно сохранения конфигурации

Для вставки конфигурации из файла необходимо выбрать узел КСК, сетевой группы, COM-порта или контроллера доступа, вызвать контекстное меню и выбрать пункт **«Загрузить из файла»** (рисунок 57).

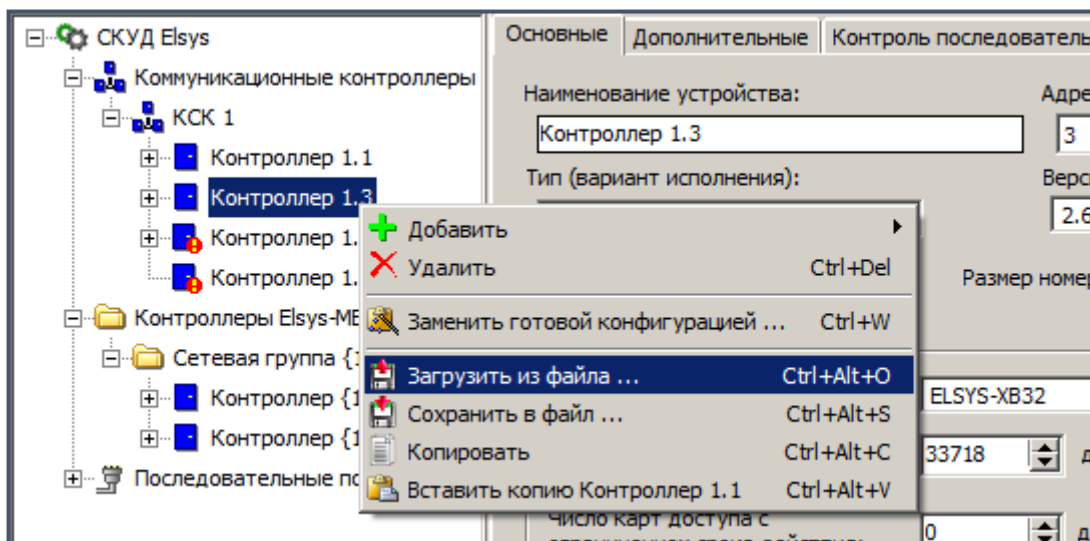


Рисунок 57 - Загрузка сохраненной конфигурации из контекстного меню контроллера

При загрузке конфигурации с заменой уже имеющейся появится окно с запросом либо замены параметров конфигурации (рисунок 53), либо на полную замену конфигурации (рисунок 54).

При загрузке новой конфигурации без замены (добавление контроллера), то после выбора загружаемой конфигурации появится окно (рисунок 58) с запросом на загрузку наименований устройств из файла.

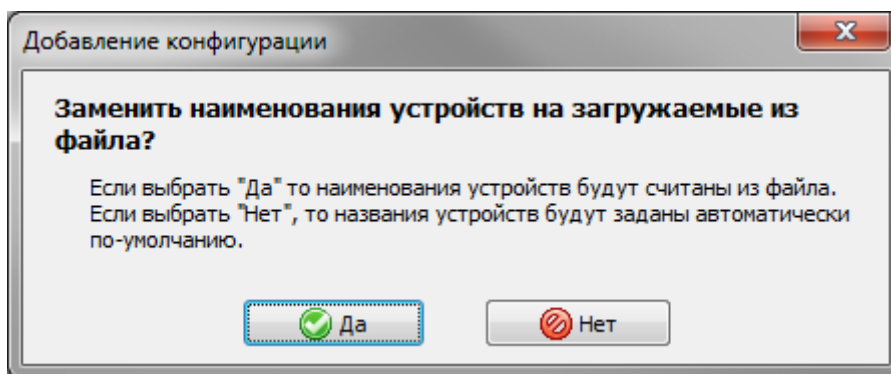


Рисунок 58 - Окно запроса загрузки наименований устройств из файла

Описанные действия могут быть также выполнены кнопками с аналогичными значками на панели дополнительных средств драйвера «Бастион-2 – Elsys» (таблица 3).

## 5.8 Настройка точек доступа

В СКУД Elsys поддерживаются программные модели следующих устройств:

- 1) дверь с односторонним контролем доступа;
- 2) дверь с двусторонним контролем доступа;
- 3) турникет;
- 4) ворота (шлагбаум).

Для корректной работы оборудования СКУД необходимо выполнить настройку точек доступа (двери, турникеты, ворота, шлагбаумы) и входящих в их состав устройств – считыватели (см. п. 5.8), входы (см. п. 5.9), выходы (см. п. 5.11). Для настройки прочих управляемых преграждающих устройств (например, шлюзов) и реализации усиленных алгоритмов доступа следует использовать систему программируемых аппаратных взаимодействий, описание которой приведено ниже.

Перед началом самостоятельной настройки оборудования СКУД рекомендуется ознакомиться с готовыми конфигурациями – весьма вероятно, что среди них будет найдено подходящее решение или основа для создания новой конфигурации.

### 5.8.1 Добавление точек доступа и считывателей

Для добавления точки доступа следует из контекстного меню узла контроллера выбрать пункт «Добавить», а затем выбрать один из пунктов, соответствующий типу точки доступа, — «Дверь», «Турникет» или «Ворота» (рисунок 59).

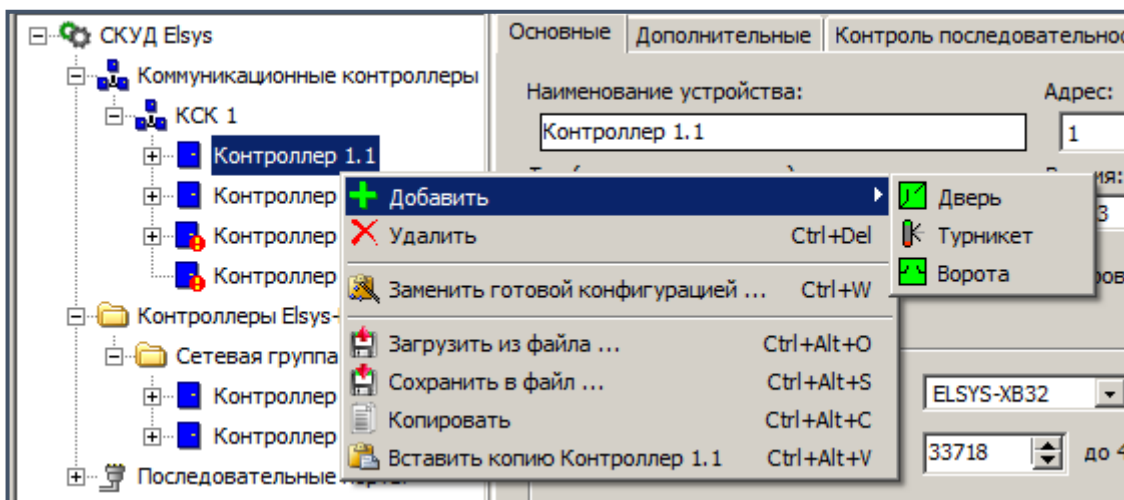


Рисунок 59 - Контекстное меню добавления точки доступа

Затем следует добавить входной считыватель, а если точка доступа двусторонняя, также и выходной считыватель (рисунок 60).

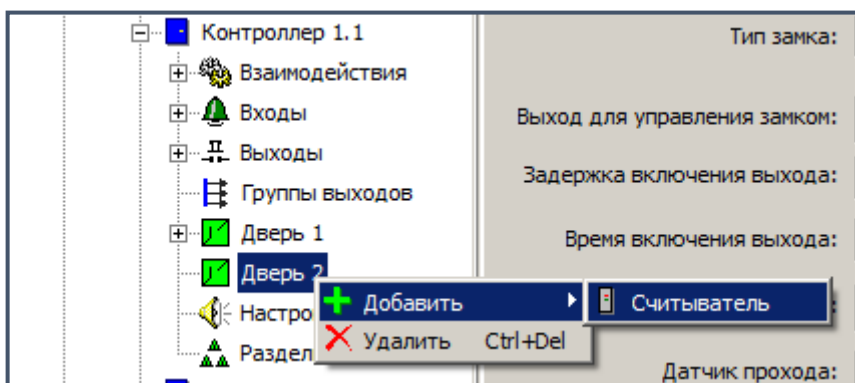


Рисунок 60 - Контекстное меню добавления считывателя

Следует учитывать, что считыватели нумеруются в порядке их добавления (в дальнейшем номер считывателя изменить нельзя), а номер считывателя соответствует его физическому подключению к плате контроллера. При необходимости можно изменить роль считывателя, сделав его входным или выходным.

Для версий контроллеров 1.35 и ниже (выпускались до 2004 года) первый считыватель (на плате контроллера обозначен как CR1, он первым добавляется в базу данных) обязательно должен быть входной, а второй (CR2) – выходной, и эти настройки по умолчанию не следует менять. Кроме того, для контроллеров этих версий недопустимо добавлять выходной считыватель при отсутствии входного.

Контроллеры варианта исполнения «PRO4» позволяют использовать до четырёх считывателей (остальные варианты исполнения – не более двух).

Прежде чем приступать к настройкам точек доступа, необходимо добавить в базу и настроить все входы и выходы, используемые в конфигурации считывателей и точек доступа. Кроме того, в базу могут быть добавлены входы и выходы, имеющие вспомогательное и самостоятельное назначение.

### 5.8.2 Настройка двери с односторонним контролем доступа

Точек доступа этого типа может быть до двух на один контроллер (для исполнения PRO4 – до четырёх).

Типовые настройки двери с односторонним контролем доступа приведены на рисунке 61.

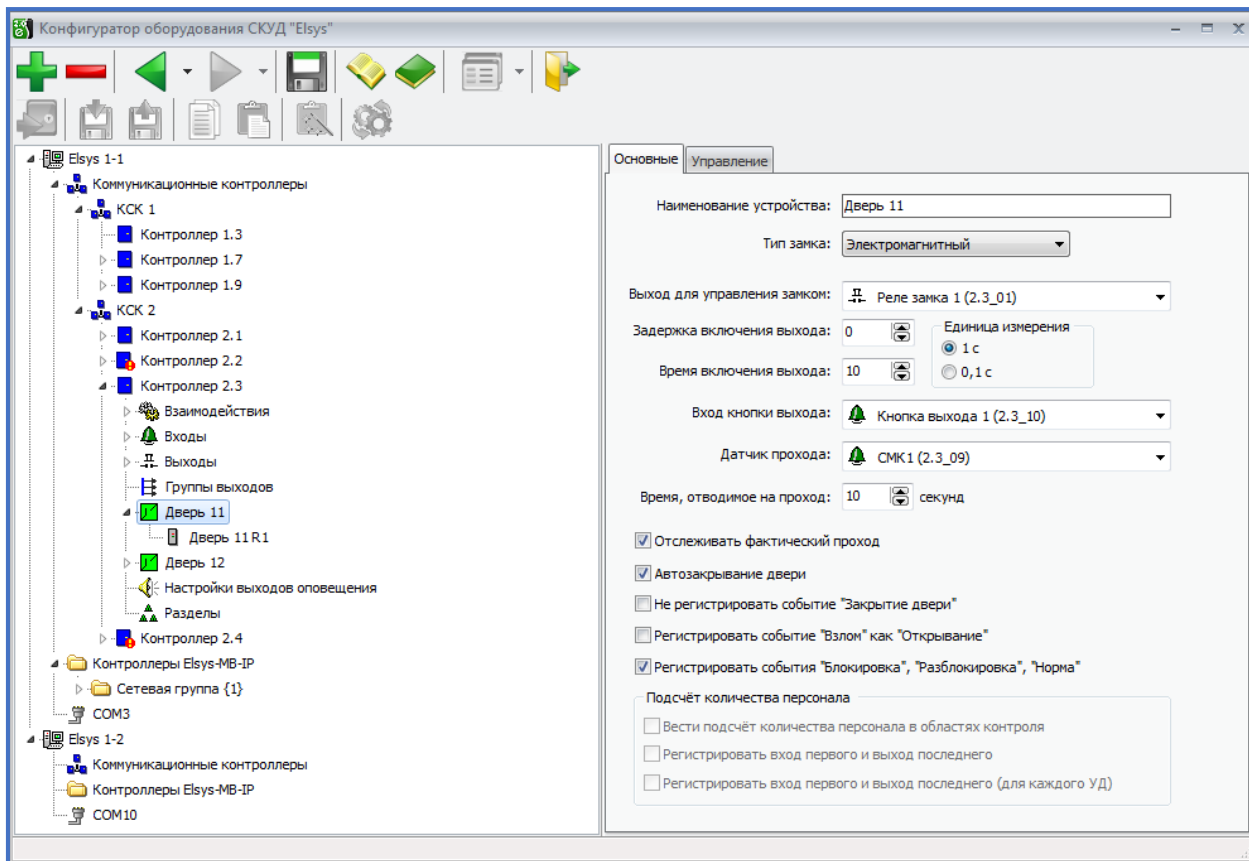


Рисунок 61 - Настройки двери с односторонним контролем доступа

При настройке необходимо предварительно добавить следующие устройства.

- Добавить входной считыватель («Дверь->Добавить->Считыватель»). У считывателей имеется ряд настроек, однако при первоначальной настройке системы их можно оставить без изменений.
- Добавить датчик прохода («Входы->Добавить->Вход», затем выбрать только добавленный вход в списке выбора «Дверь->Свойства->Датчик прохода»). Настроить вход в соответствии с его схемой подключения (как правило, нормально замкнутый без оконечного резистора, время интегрирования 300 мс).

**Внимание!** Если вход датчика прохода настроить неверно, точка доступа будет работать неправильно!

Остальные опции входа здесь роли не играют, их настраивать не нужно.

- Добавить кнопку выхода. Кнопка запроса на выход выбирается в списке выбора «Дверь->Свойства->Вход кнопки выхода». Обычные настройки – 70 мс, нормально разомкнутый, без оконечного резистора;

- Добавить выход для управления замком (**«Выходы->Добавить->Выход»**). Следует выбирать любой из выходов контроллера, обычно релейный. Обычно никаких дополнительных настроек для выхода не требуется.

Настройка **«Тип замка»** имеет два значения - **«Электромеханический»** и **«Электромагнитный»**.

Выбирать тип **«Электромеханический»** следует, если замок электромеханический (после подачи отпирающего импульса дверь, оборудованная таким замком, остаётся фактически незапертой, и для приведения двери в закрытое состояние её необходимо открыть и снова закрыть).

Во всех остальных случаях следует выбирать тип **«Электромагнитный»**. Всё различие в алгоритмах работы заключается в том, что для электромеханического замка может формироваться сообщение «Дверь не заперта» (если по истечении отводимого времени не был совершён проход), а в режиме разблокировки дверь после закрытия будет автоматически отпираться.

**«Задержка включения выхода»** в большинстве случаев устанавливается в 0.

**«Время включения выхода»** для электромеханического замка устанавливается обычно минимальным (0,1 – 1 с), кроме того, рекомендуется использовать RC-цепочку, встроенную в источник питания контроллера (схема её подключения и рекомендации по использованию приведены в Руководстве по эксплуатации СКУД Elsys). Для электромагнитного замка параметр **«Время включения выхода»** обычно устанавливается в диапазоне 5 – 30 сек.

**«Время шунтирования датчика прохода»** - это, фактически, время, отводимое на проход. Обычно устанавливается в диапазоне 5 – 30 сек. Если замок электромагнитный, то настройка «Время шунтирования датчика прохода» должна иметь значение, равное или чуть большее, чем «Время включения выхода».

**«Автозакрывание двери»** - режим при котором по факту закрытия двери досрочно выключается замок и берётся под охрану датчик прохода.

**«Отслеживать фактический проход»** - регистрация прохода по срабатыванию датчика прохода.

**«Не регистрировать событие «Закрытие двери»** - обычно должна быть выключена, так как это событие используется для изменения состояния пиктограммы двери.

**«Регистрировать событие «Взлом» как «Открывание»** - обеспечивает замену события «Взлом» событием «Открывание двери» при регистрации в протоколе.

**«Регистрировать события «Блокировка», «Разблокировка», «Норма»** - при включении данной опции, в протоколе регистрируются соответствующие события.

**«Единица измерения»** - настройка, задающая единицу измерения (0,1 с или 1 с) для управления выходом замка, т. е. является множителем для опций **«Задержка включения замка»** и **«Время включения замка»**.

«Подсчёт количества персонала» - группа параметров, которая используется для подсчёта количества персонала в областях контроля. Возможность подсчёта персонала доступна в двусторонних точках прохода при включенной опции контроллера «Расширенные возможности настройки» и выключенном временном контроле последовательности прохода в контроллере (рисунок 62).

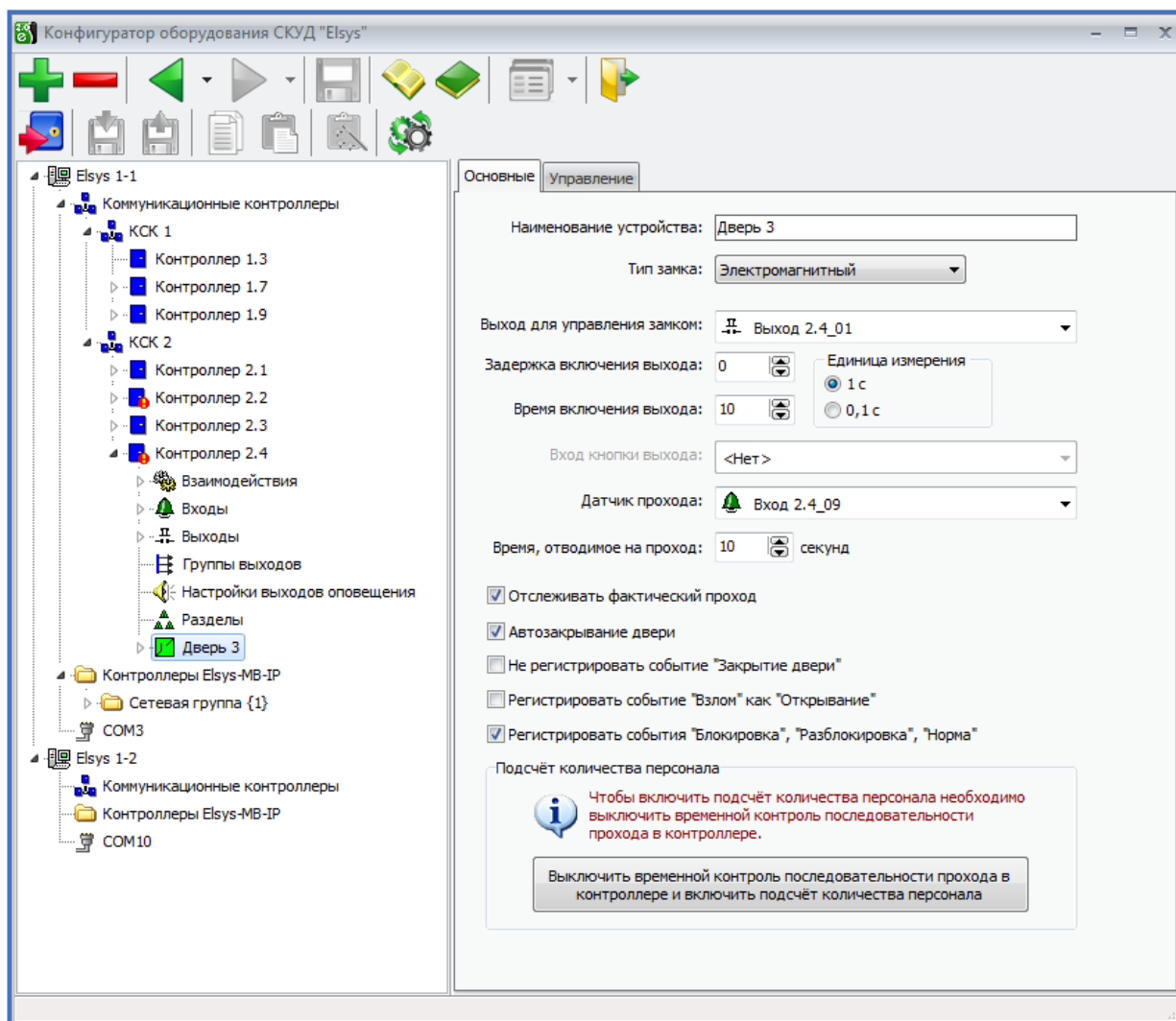


Рисунок 62 – Свойства двери при включенном контроле последовательности прохода в контроллере

Вкладка «Управление» позволяет управлять дверью непосредственно из окна конфигуратора, (более подробно см. п. 5.16).

### 5.8.3 Настройка двери с двусторонним контролем доступа

Контроллеры Elsys-MB могут обслуживать либо одну (исполнения «PRO», «Standard», «Light»), либо две («PRO4») двусторонних двери.

Для настройки двусторонней двери необходимо добавить и назначить:

- два считывателя (первый – входной, второй – выходной);
- СМК;
- выход для управления замком.



Назначение остальных настроек двухсторонней двери аналогично настройкам для односторонней двери, описанным в п. 5.8.2.

#### 5.8.4 Настройка турникета

Контроллеры Elsys-MB позволяют обслуживать от одного (исполнения «PRO», «Standard», «Light») до двух («PRO4») турникетов.

Программная модель турникета фактически состоит из двух половин, идентичных двери (рисунок 63).

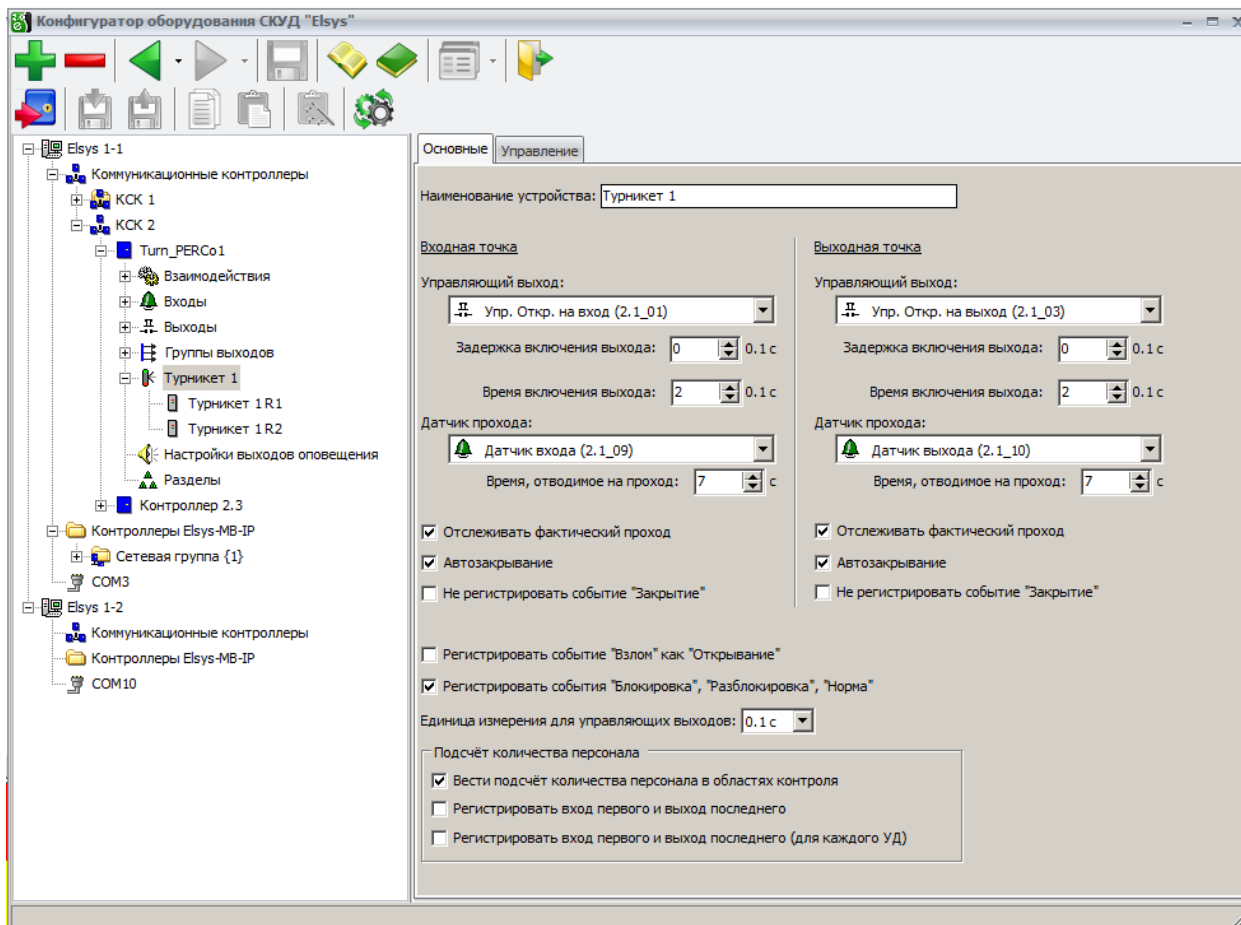


Рисунок 63 - Настройки турникета

Как и для двусторонней двери, необходимо добавить и настроить два считывателя. Турникет имеет два датчика прохода, два выхода управления проходом и две группы настроек, аналогичных двери. Следует помнить, что для модели турникета отсутствует встроенная реализация команд «Разблокировка», «Блокировка», «Нормальный режим» (их реализация специфична в зависимости от конкретной модели турникета). Эти команды могут быть настроены с помощью аппаратных взаимодействий (см. п. 9.1).

В подавляющем большинстве случаев настройки, соответствующие **«Входной»** и **«Выходной»** частям турникета (кроме настроек **«Выход для управления замком»** и **«Датчик прохода»**), должны быть идентичны.

Обычно для отпирания турникета используется короткий импульс (**«Время включения выхода»** следует установить равным 0,2 с). Время шунтирования дверного контакта

обычно следует устанавливать чуть больше, чем время, отводимое на проход, формируемое электроникой турникета (обычно 5-7 сек).

Настройки **«Отслеживать фактический проход»** и **«Автозакрывание»** в большинстве случаев должны быть включены, а настройки **«Не регистрировать закрытие»** - выключены (если не используются пиктограммы турникета, последнюю опцию можно включить, при этом события «Турникет закрыт» регистрироваться не будут).

Большинство турникетов имеет отдельный датчик прохода для каждого направления. Так как импульс, формируемый электроникой турникета в момент прохода, может быть очень коротким, время интегрирования соответствующих входов следует устанавливать равным 0 мс. Для установки типа входа (нормально замкнутый или нормально разомкнутый) следует ознакомиться с инструкцией на турникет.

**«Подсчёт количества персонала»** - группа параметров, которая используется для подсчёта количества персонала в областях контроля. Возможность подсчёта персонала доступна при включенной опции контроллера «Расширенные возможности настройки» и при выключенном временном контроле последовательности прохода в контроллере.

Вкладка **«Управление»** позволяет управлять турникетом непосредственно из окна конфигуратора, (более подробно см. п. 5.16).

### 5.8.5 Настройка ворот и шлагбаумов

Несмотря на различие этих преграждающих устройств и многообразие алгоритмов управления ими, наиболее общие их свойства были включены в программную модель ворот контроллеров Elsys-MB. Каждый контроллер может обслуживать до двух ворот (вариант исполнения «PRO4» – до четырёх). Однако, при выборе оборудования следует учитывать, что для управления одними воротами может потребоваться до трёх релейных выходов.

Окно настройки ворот изображено на рисунке 64.

**«Датчик закрытого состояния»** - вход, используемый для мониторинга состояния ворот (взлом, фактический проход, закрыто и т. п.). Аналог датчика прохода двери и турникета.

Назначение опций **«Имя устройства»**, **«Время шунтирования датчика закрытого состояния»**, и **«Отслеживать фактический проход»** соответствует назначению аналогичных опций для двери и турникета.



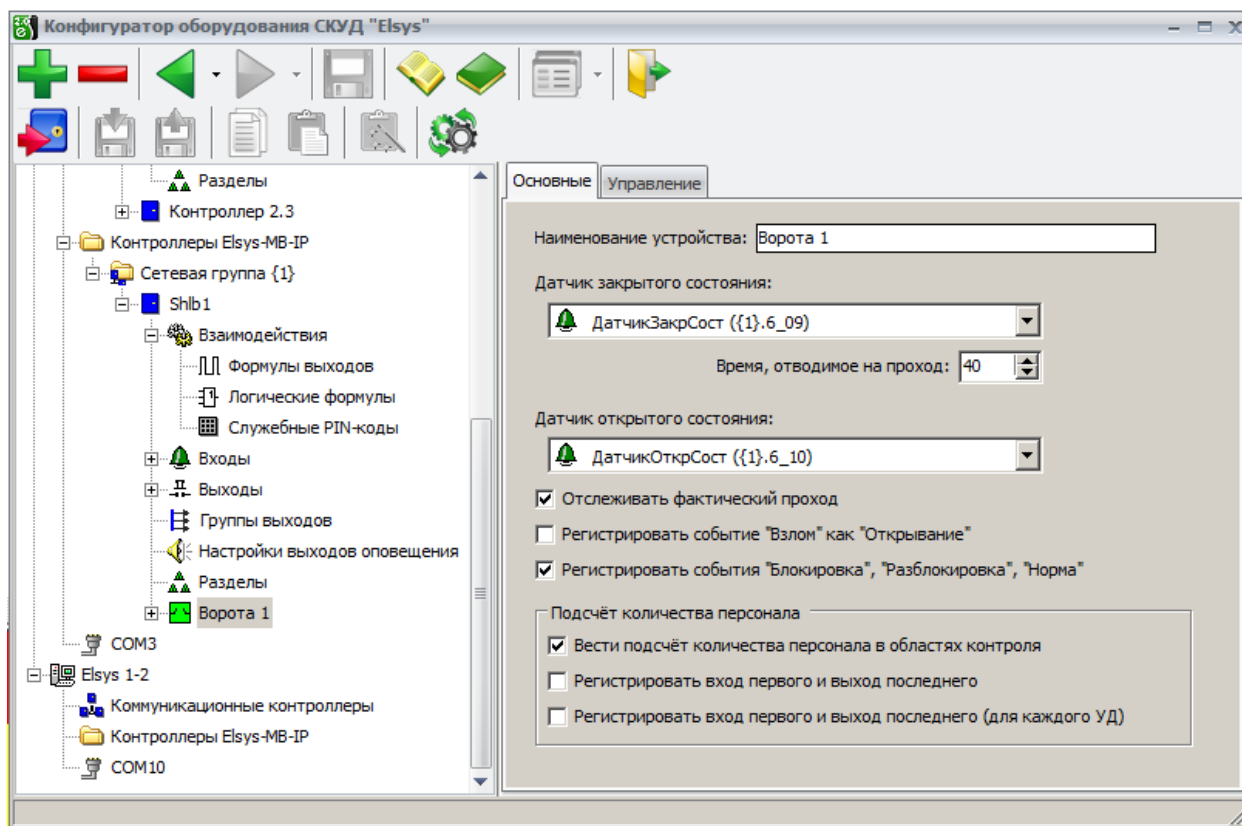


Рисунок 64 - Настройки ворот

«**Датчик открытого состояния**» - вход контроллера, используемый для контроля состояния ворот «Открыто полностью».

Ворота и шлагбаумы имеют три физических состояния, отображаемых на пиктограммах устройств, – закрыто, приоткрыто и открыто полностью. Возможность их мониторинга зависит от конкретной модели исполнительного устройства. «Норма» для датчика закрытого состояния соответствует состоянию ворот «Закрыто». Если ворота штатно открыты и датчик закрытого состояния имеет состояние «Не норма», то состояние ворот, сообщаемое контроллером, зависит от наличия или состояния датчика открытого состояния ворот (если отсутствует или в тревоге – ворота имеют состояние «Открыто полностью», а если в норме – состояние ворот будет «Приоткрыто»).

Для управления приводами ворот и шлагбаумов в ПО «Бастион-2» предусмотрены три основные команды: «Открыть», «Закрыть» и «Стоп». Ввиду многообразия устройств, представленных на рынке, реализация этих команд в контроллерах Elsys-MB никак не стандартизирована, а должна настраиваться при помощи аппаратных взаимодействий (см. п. 9.1). Следует помнить, что предоставление доступа на вход или на выход автоматически формирует команду «Открыть».

По умолчанию пиктограмма ворот имеет обычный для этого типа устройств вид. Если необходимо использовать пиктограмму шлагбаума, при настройке карт следует выбрать в свойствах пиктограммы «**Вид 2**» (рисунок 65).

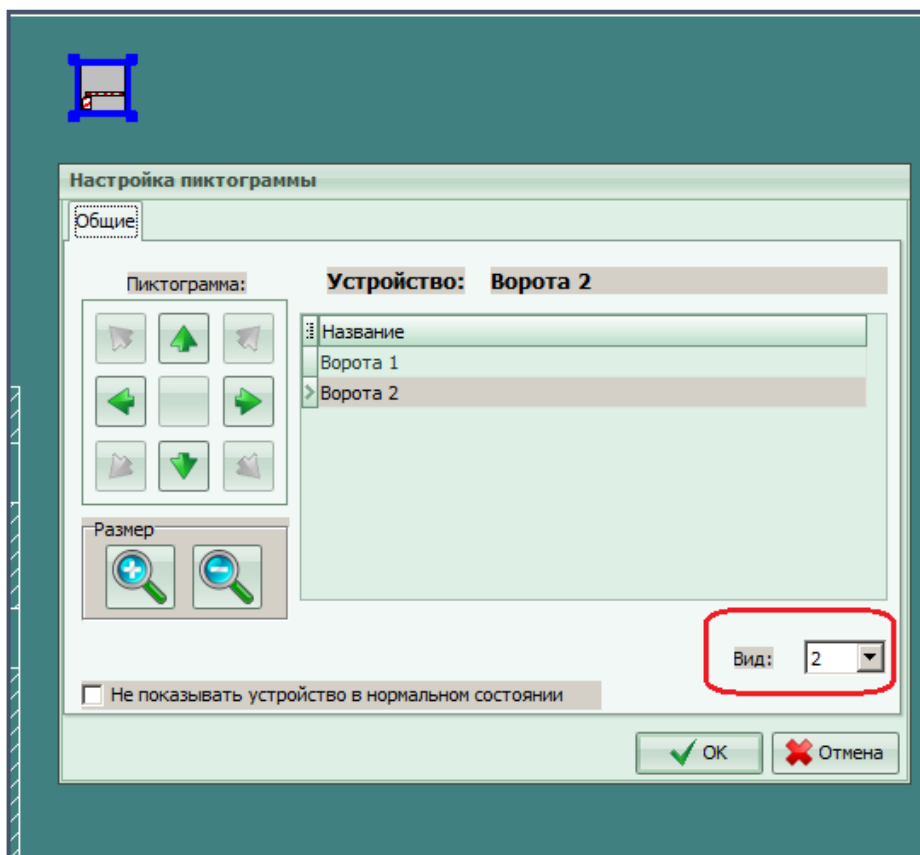


Рисунок 65 - Настройка вида пиктограммы ворот для отображения шлагбаума

Вкладка **«Управление»** позволяет управлять воротами или шлагбаумом непосредственно из окна конфигуратора, (более подробно см. п. 5.16).

## 5.9 Настройка входов

### 5.9.1 Описание настроек входов

Для добавления входа необходимо выбрать узел **«Входы»** и вызвать контекстное меню, в котором выбрать пункт **«Добавить»** и далее выбрать **«Вход»** (рисунок 66).

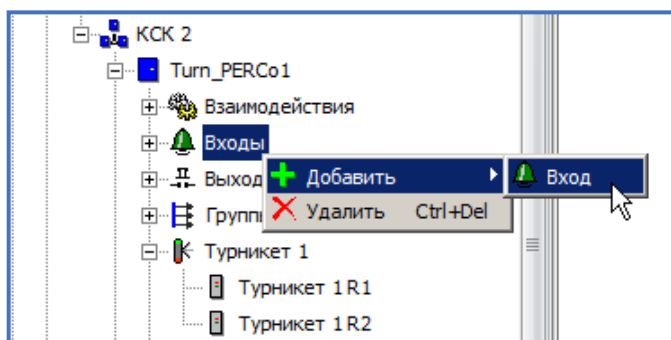


Рисунок 66 - Контекстное меню добавления входа

В дерево устройств будет добавлен вход с первым свободным номером. В правой части окна конфигуратора появится окно параметров аналогового или цифрового входа (рисунок 67).

Номер входа соответствует его физическому расположению на плате контроллера и его типу. Входы с номерами 1 – 8 – аналоговые, с номерами 9 – 21 – цифровые.

Если вход используется в конфигурации двери, турникета или считывателя, играет роль лишь группа настроек «Тип входа» и параметр «Время интегрирования». Возможные комбинации настроек в группе «Тип входа» зависят от того, какой вход настраивается – аналоговый или цифровой.

Основные | Управление

Наименование устройства:  Номер входа:  (Аналоговый вход)

Тип входа

Нормально разомкнутый

Нормально замкнутый

С оконечным резистором 2 кОм

Дополнительные параметры для ШС с оконечным резистором:

Анализировать 10% отклонение сопротивления

Наличие дополнительных резисторов

Схема №3: Норма/На охране -  $R_{ш} = 1..3 \text{ кОм}$ ; Неготовность/Тревога -  $R_{ш} < 0,75 \text{ кОм}$  или  $R_{ш} > 4,5 \text{ кОм}$

Параметры входа

Тип шлейфа сигнализации:

Всегда на охране

Фиксировать тревогу

Автоматическая постановка на охрану из состояния "Невзято"

Автоматическая постановка на охрану из состояния "Тревога"

через:  секунд

Задержка взятия на охрану, с:

Задержка тревоги, с:

Время интегрирования, мс:

Время восстановления, с:

Параметры протоколирования событий

Отслеживать состояние вне охраны

Не протоколировать события

Рисунок 67 - Окно параметров входа

Всего возможно 8 комбинаций параметров (нормально замкнутый, нормально разомкнутый, нормально замкнутый с оконечным резистором, нормально разомкнутый с оконечным резистором, оба типа датчиков с оконечным резистором, нормально замкнутый с оконечным резистором и добавочными резисторами, нормально разомкнутый с оконечным резистором и добавочными резисторами, оба типа датчиков с оконечным резистором и добавочными резисторами). В большинстве применений, не

связанных с охранными функциями, обычно используются два режима – нормально замкнутый (СМК, датчики прохода большинства турникетов) и нормально разомкнутый (большинство кнопок управления). Другие 6 режимов (с оконечным резистором) возможны только для аналоговых входов и используются реже.

**«Время интегрирования»** – время, в течение которого контроллер детектирует переход входа из одного физического состояния в другое. Допустимые значения параметра - 0, 70 или 300 мс (по умолчанию).

Устанавливать время интегрирования следует из следующих соображений:

**0 мс** – для датчиков прохода турникетов и прочих устройств, выдающих короткий импульсный сигнал (длительностью 20..100 мс);

**70 мс** - для кнопок управления и большинства подобных применений (защита отдребезга контактов);

**300 мс** – для охранных входов и датчиков открывания двери (защита от ложных срабатываний).

Группа параметров **«Параметры входа»** устанавливает совокупность параметров входа в зависимости от типа шлейфа сигнализации.

**«Тип шлейфа сигнализации»** - опция задаёт логику работы входа в зависимости от выбранного типа ШС. Описание возможных значений этой настройки приведено в таблице 5.

Настройки **«Всегда на охране»** и **«Фиксировать тревогу»** актуальны, если вход имеет тип ШС «Вход общего назначения» и для него не назначена специальная функция (датчик прохода, кнопка управления охраной и т. п.).

**Таблица 5 – Варианты настройки «Тип шлейфа сигнализации»**

<b>Тип ШС - «Вход общего назначения»</b>
<p>Это значение настройки обеспечивает совместимость с конфигурациями, созданными в предыдущих версиях. Настройка «Тип ШС» принудительно устанавливается в значение «Вход общего назначения» и недоступна для редактирования в следующих случаях:</p> <ul style="list-style-type: none"><li>• контроллер имеет версию ниже 2.60;</li><li>• отсутствует модуль расширения памяти;</li><li>• вход имеет специальное назначение (является датчиком прохода и др.).</li></ul> <p>Только для этого типа ШС, при включенной опции <b>«Всегда на охране»</b> возможны состояния ШС «Обрыв» и «КЗ».</p> <p>Вход, имеющий тип ШС <b>«Вход общего назначения»</b>, не может быть включён в раздел.</p> <p>Для задания логики работы входа, имеющего этот тип ШС, следует использовать настройки <b>«Всегда на охране»</b> и <b>«Фиксировать тревогу»</b>.</p>

Таблица 5 – Варианты настройки «Тип шлейфа сигнализации»

<b>Тип ШС - «Охранный»</b>
<p>Установка типа «Охранный» предусматривает использование входа в охранной подсистеме. При нарушении взятый на охрану ШС немедленно переходит в состояние «Тревога». Состояние «Тревога» сохраняется до тех пор, пока вход не будет снят с охраны или повторно взят на охрану.</p> <p>Для ШС этого типа недоступна настройка «Задержка тревоги» и недоступны некоторые состояния, связанные с этим режимом.</p>
<b>Тип ШС - «Входной»</b>
<p>Установка типа «Входной» предусматривает использование входа в охранной подсистеме. Этот тип следует назначать для ШС, к которым подключены датчики проникновения в помещение, например магнитоконтактные сигнализаторы, устанавливаемые на дверях. Вход может быть включён в раздел. Свойства входа аналогичны типу «Охранный», однако у входа имеется также настройка «Задержка тревоги». Если она ненулевая, при нарушении ШС сначала будет сформировано событие «Нарушение входной зоны», а затем, если в течение заданного времени ШС не будет снят с охраны, он перейдёт в состояние «Тревога».</p> <p>Если в состав раздела (см. ниже) включена дверь, соответствующая ей охранная зона имеет тип ШС «Входной». Ряд настроек, актуальных для этого типа ШС («Задержка взятия», «Задержка тревоги», «Автоматическая постановка из тревоги» и др.), следует настраивать в свойствах входа, к которому подключен датчик прохода двери.</p> <p>На логику работы двери в подсистеме СКУД эти настройки не влияют.</p> <p>Обычно для ШС типа «Входной» используется задержка взятия и задержка тревоги, необходимые в том случае, если управление режимами охраны осуществляется изнутри помещения (с внутреннего считывателя двусторонней двери).</p>
<b>Тип ШС - «Объем»</b>
<p>Установка типа «Объем» предусматривает использование входа в охранной подсистеме. Тип ШС «Объем» следует назначать тем ШС, в которые включены объёмные извещатели и иные датчики присутствия человека. ШС, аналогичный по своим основным свойствам ШС типа «Охранный». Если ШС не входит в состав раздела, его работа полностью идентична работе ШС типа «Охранный». Логика работы типа ШС «Объем» взаимосвязана с состоянием ШС типа «Входной», входящих в тот же раздел.</p>
<b>Тип ШС - «Круглосуточный»</b>
<p>Установка типа «Круглосуточный» предусматривает использование входа в охранной подсистеме. ШС, который нельзя снять с охраны (команда снятия с охраны сбрасывает тревогу). ШС такого типа часто целесообразно включать в раздел, для упрощения реализации индикации состояния и управления сбросом тревоги.</p>

**«Всегда на охране»** – эту опцию следует включать, если необходимо ограничить число состояний входа двумя – «Тревога» и «На охране». Это наиболее часто используемый режим работы входов контроллера, опция используется для ШС «Вход общего назначения».

**«Фиксировать тревогу»** – при включенной опции состояние входа остается тревожным до прихода подтверждающего сообщения (снятие с охраны, повторная постановка на охрану). Опция используется для ШС «Вход общего назначения».

В таблице 6 описана логика работы входа с типом ШС «Вход общего назначения» при всех возможных значениях опций «Всегда на охране» и «Фиксировать тревогу».

**Таблица 6 – Логика работы входа с типом ШС «Вход общего назначения» для различных комбинаций опций «Всегда на охране» и «Фиксировать тревогу»**

Опция «Всегда на охране»	Опция «Фиксировать тревогу»	Краткое описание режима работы входа
Выключена	Выключена	Если вход на охране, у него возможны состояния «Тревога» и «На охране». Если вход снят с охраны, возможны также состояния – «Норма - готовность» и «Неготовность».
Включена	Выключена	Основные состояния входа – «Тревога» и «На охране». Для аналоговых входов возможна регистрация состояний «Обрыв» и/или «Короткое замыкание». Рекомендуется для большинства применений, не связанных с охранными функциями.
Включена	Включена	Функционирование ШС «Вход общего назначения» аналогично работе ШС типа «Круглосуточный»
Выключена	Включена	Функционирование ШС «Вход общего назначения» аналогично работе ШС типа «Охранный»

**«Время восстановления»** – параметр, определяющий время задержки перехода входа из состояний «Тревога», «Неготовность» в состояния «Норма – готов к постановке на охрану», «На охране». Диапазон допустимых значений от 0 до 127 с. Этот параметр актуален для ШС типа «Вход общего назначения», у которых выключена настройка «Фиксировать тревогу».

При использовании контроллеров «Elsys-MB» версии 2.60 и старше с установленным модулем расширения памяти для входов возможно задание типа ШС, отличного от значения «Вход общего назначения» и становится доступным ряд настроек, предназначенных для использования в охранной подсистеме.

**«Автоматическая постановка на охрану из состояния «Невзято»** - опция обеспечивает автоматический переход входа из состояния «Невзято» в состояние «На охране», если ШС будет пребывать в нормальном состоянии более 3 с. Эта опция актуальна для следующих типов ШС: «Охранный», «Входной» и «Объем».

**«Автоматическая постановка на охрану из состояния «Тревога»** - опция обеспечивает автоматический переход входа из состояния «Тревога» в состояние «На охране» через указанный интервал времени из диапазона от 0 до 1250 с. Опция может использоваться для всех типов ШС кроме типа «Вход общего назначения».

**«Задержка взятия на охрану»** - настройка позволяет установить интервал времени из диапазона от 0 до 255 с, в течение которого вход находится, в зависимости от его физического состояния, в одном из состояний «Задержка взятия – готовность», «Задержка взятия - неготовность». Обычно задержка взятия используется для входных ШС, если постановка на охрану осуществляется изнутри помещения, а затем сотрудник выходит из помещения. Настройка доступна для ШС «Охранный», «Входной» и «Объем». Для объёмных ШС задержка необязательна, т. к. ШС этого типа шунтируются, пока продолжается задержка на входном ШС.

**«Задержка тревоги»** - настройка позволяет установить интервал времени из диапазона от 0 до 255 с, в течение которого вход находится, в зависимости от его физического состояния, в одном из состояний «Задержка тревоги – готовность», «Задержка взятия - неготовность». Обычно задержка тревоги используется для входных ШС, если снятие с охраны осуществляется внутри помещения. Настройка доступна только для ШС типа «Входной».

**«Отслеживать состояние вне охраны»** – при включенной опции состояние входа отслеживается, даже если вход не взят под охрану. Если вход охраняемый, опцию включать обычно не следует (так как зона, если снята с охраны, нарушаться может многократно, а важной информации такое событие не несёт).

**«Не протоколировать события»** – при установленной опции события об изменении состояния входа не будут регистрироваться и передаваться контроллером.

Вкладка **«Управление»** позволяет управлять входом непосредственно из окна конфигуратора (более подробно см. п. 5.16).

**«Раздел»** - раздел, в который включён ШС. В раздел могут быть включены ШС всех типов кроме типа «Вход общего назначения». Если вход включен в какой-либо раздел, команды управления его состоянием «Поставить на охрану» и «Снять с охраны» становятся недоступными как извне, так и через взаимодействия. Если вход входит в состав раздела, им можно управлять только через команды управления разделом.

### 5.9.2 Использование входов

Входы контроллера могут находиться в одном из физических состояний: «Нарушено», «Норма», «Обрыв», «Короткое замыкание». В зависимости от настроек входа и режима его работы, вход может находиться в одном из логических состояний, приведённых в таблице 7. Возможные для каждого типа ШС состояния отмечены знаком «+».

Состояния «Обрыв» и «Короткое замыкание» возникают при физических состояниях ШС, соответствующим неисправностям. Эти состояния возможны только для ШС типов 1.3, 1.4. Одновременно с регистрацией этих состояний в протоколе регистрируются одноимённые события.



Состояния «Норма – готовность» (соответствует физическому состоянию «Норма») и «Неготовность» (соответствует физическому состоянию «Нарушение») характеризуют состояние входа, снятого с охраны. Эти состояния могут регистрироваться как в момент изменения физического состояния входа (при этом регистрируются одноимённые события), так и в случае снятия ШС с охраны (при этом регистрируется событие «Снятие с охраны»).

Таблица 7 – Возможные логические состояния входов

№	Состояние	Тип ШС							
		1.1	1.2	1.3	1.4	2	3	4	5
1	«Обрыв»	–	–	+	+	–	–	–	–
2	«Короткое замыкание»	–	–	+	+	–	–	–	–
3	«Норма – готовность»	+	+	–	–	+	+	+	–
4	«Неготовность»	+	+	–	–	+	+	+	–
5	На охране	+	+	+	+	+	+	+	+
6	Задержка взятия - готовность	–	–	–	–	+	+	+	–
7	Задержка взятия - неготовность	–	–	–	–	+	+	+	–
8	Невзятие	–	–	–	–	+	+	+	–
9	Задержка тревоги	–	–	–	–	–	+	+	–
10	«Удержание»	+	–	–	–	–	–	–	–
11	«Тревога»	+	+	+	+	+	+	+	+

**Примечание.** В таблице условно обозначены типы ШС:

**1.1** – «Вход общего назначения», опция «Всегда на охране» - выключена, опция «Фиксировать тревогу» - выключена

**1.2** – «Вход общего назначения», опция «Всегда на охране» - выключена, опция «Фиксировать тревогу» - включена

**1.3** – «Вход общего назначения», опция «Всегда на охране» - включена, опция «Фиксировать тревогу» - выключена

**1.4** – «Вход общего назначения», опция «Всегда на охране» - включена, опция «Фиксировать тревогу» - включена

**2** – «Охранный»,

**3** – «Входной»,

**4** – «Объём»,

**5** – «Круглосуточный».

Здесь и далее в этом документе используются эти сокращённые обозначения типа ШС.



Состояние «На охране» и одноимённое событие регистрируются в момент постановки ШС на охрану, если он до этого находился в состоянии «Норма - готовность». Также, при определённых настройках ШС возможен переход в состояние «На охране» из состояний «Тревога», «Невзятие», «Задержка взятия – готовность».

Если ШС в момент постановки на охрану находился в состоянии «Неготовность», будет сформировано событие «Невзятие на охрану», а ШС, в зависимости от настроек, может либо сохранить своё состояние, либо перейти в одно из состояний – «Задержка взятия - неготовность» или «Невзятие». Состояние «Задержка взятия - неготовность» будет сформировано, если вход имеет значение настройки «Задержка взятия на охрану», отличное от нуля. Состояние «Невзятие» будет сформировано, если у входа включена настройка «Автоматическое взятие на охрану поле невзятия».

Если ШС имеет отличную от нуля задержку взятия, то в момент постановки на охрану, в зависимости от его физического состояния, будет сформировано состояние «Задержка взятия - готовность» (если ШС был в норме) либо «Задержка взятия - неготовность» (если ШС был нарушен). До истечения задержки взятия ШС может многократно нарушаться и восстанавливаться, переходя из одного вышеописанного состояния в другое. Если вход, находившийся в состоянии «Задержка взятия на охрану», по истечении задержки взятия останется в нарушенном состоянии, он перейдёт в состояние «Тревога», а если он имеет тип ШС «Входной» и ненулевую задержку тревоги – в состояние «Задержка тревоги». Если вход по истечении задержки взятия находится в состоянии «Норма», он перейдёт в состояние «На охране».

В случае нарушения ШС, находящегося на охране, и имеющего любой тип, кроме типа «Входной», будет немедленно сформировано состояние «Тревога» (с одновременной регистрацией события «Тревога»). Если был нарушен ШС, находящийся на охране и имеющий тип «Входной», этот ШС перейдёт в состояние «Задержка тревоги» и будет сформировано событие «Тревога входной зоны».

Вход, находящийся в состоянии «Задержка тревоги», должен быть в течение времени задержки тревоги снят с охраны, в противном случае он перейдёт в состояние «Тревога».

Вход, находящийся в состоянии «Тревога» и имеющий тип ШС 2 – 5 остаётся в этом состоянии, вне зависимости от его физического состояния, до тех пор, пока не будет выполнено снятие с охраны или повторная постановка на охрану. Аналогичным образом функционирует вход, имеющий тип ШС «Вход общего назначения» и включенную опцию «Фиксировать тревогу».

Если вход имеет тип ШС «Вход общего назначения» и выключенную настройку «Фиксировать тревогу» (тип 1.1 или 1.3), в случае восстановления нормального состояния, он немедленно перейдёт в состояние «На охране». Если задано отличное от нуля значение настройки «Время восстановления», переход из состояния «Тревога» в состояние «На охране» произойдёт не сразу, а спустя заданное время.

Состояние «Удержание» возможно только для ШС типа 1.1. Если для такого входа выполняется команда «Снять с охраны на время», а по истечении этого времени он оказался в нарушенном состоянии, будет сформировано состояние «Удержание».

### 5.9.3 Особенности настройки входов в зависимости от их функционального назначения

В таблице 8 описаны особенности настройки входов в зависимости от их функционального назначения.

**Таблица 8 – Рекомендуемые настройки входов в зависимости от их функционального назначения**

№	Функциональное назначение входа	Рекомендуемые настройки
1	Вход используется для подключения считывателя (IN9 – IN12, IN16 – IN19), датчика вскрытия корпуса (IN20) или сигнала PWFAIL (IN21)	Входы, занятые считывателями, никаких настроек не требуют и в конфигурации недоступны. Если включены опции <b>«Использовать тампер»</b> и <b>«Использовать мониторинг сетевого питания»</b> , входы IN20 и IN21 никаких настроек не требуют и добавлять их в конфигурацию не нужно.
2	Для входа назначена специальная функция в составе точки доступа или считывателя.	Для входа в соответствии с электрической схемой подключения и особенностями использования следует задать следующие настройки: <ul style="list-style-type: none"> <li>• <b>«Тип входа»;</b></li> <li>• <b>«Наличие оконечного резистора» ;</b></li> <li>• <b>«Наличие дополнительных резисторов» ;</b></li> <li>• <b>«Типы подключаемых датчиков»;</b></li> <li>• <b>«Время интегрирования».</b></li> </ul> Если вход используется для подключения датчика прохода, актуальна также настройка <b>«Время восстановления»</b> . Остальные настройки входа не учитываются.
3	Вход используется как вход общего назначения для подключения кнопок, контактов реле, и т. п.	Настройка <b>«Тип ШС»</b> должна иметь значение <b>«Вход общего назначения»</b> . Настройка <b>«Фиксировать тревогу»</b> должна быть выключена (тип ШС в соответствии с таблицей 7): <b>1.1</b> и <b>1.2</b> . Настройку <b>«Всегда на охране»</b> в большинстве случаев целесообразно включить, если иное не предусмотрено логикой работы.
4	Вход используется как охранный в режиме совместимости с версиями 2.55 и ниже.	Настройка <b>«Тип ШС»</b> должна иметь значение <b>«Вход общего назначения»</b> . Настройка <b>«Фиксировать тревогу»</b> должна быть включена. Если опция <b>«Всегда на охране»</b> выключена, вход работает как охранный (тип 1.3), а если включена – как круглосуточный (тип 1.4). При этом недоступен ряд настроек,

**Таблица 8 – Рекомендуемые настройки входов в зависимости от их функционального назначения**

№	Функциональное назначение входа	Рекомендуемые настройки
		<p>предназначенных для использования в охранной подсистеме (см. ниже).</p> <p>Этот режим следует использовать при отсутствии модуля расширения памяти либо при использовании конфигурации, предназначенной для версий ниже 2.60.</p>
5	Вход используется для подключения охранного ШС и может быть включен в раздел	<p>Настройка <b>«Тип ШС»</b> должна иметь значение отличное от значения <b>«Вход общего назначения»</b> (тип ШС: <b>2..5</b> в соответствии с таблицей 7). Вход может быть включен в состав раздела. Доступны такие настройки, как:</p> <ul style="list-style-type: none"> <li>• <b>«Автоматическая постановка на охрану из состояния «Не взято»;</b></li> <li>• <b>«Автоматическая постановка на охрану из состояния «Тревога»;</b></li> <li>• <b>«Задержка автоматической постановки на охрану из состояния «Тревога»;</b></li> <li>• <b>«Задержка тревоги»;</b></li> <li>• <b>«№ раздела».</b></li> </ul>

## 5.10 Настройка охранных функций

### 5.10.1 Структура охранной подсистемы

Охранная зона – часть охраняемого объекта, контролируемая одним шлейфом охранной сигнализации. В шлейф сигнализации (далее – ШС) может быть включено от одного до нескольких десятков датчиков охранной сигнализации (датчики разбития стекла, объёмные инфракрасные извещатели, магнитоконтактные сигнализаторы и т. д.), имеющих нормальнозамкнутые или нормальноразомкнутые контакты.

ШС, используемые в охранной подсистеме, могут быть подключены к любому из входов контроллера с номерами 1 – 15 (AIN1 – AIN8, IN9 – IN15). Настоятельно рекомендуется использовать для подключения ШС аналоговые входы AIN1 – AIN8, в которых предусмотрена возможность подключения оконечного резистора, обеспечивающего антисаботажную защиту.

ШС, относящиеся к одному контроллеру, могут быть сгруппированы в разделы. Раздел – логическое объединение нескольких ШС для совместного управления, взаимодействия и мониторинга. В состав раздела в качестве ШС могут входить, кроме входов № 1 – 15, также двери №№ 1 – 4. Ворота и турникеты в раздел включены быть не могут. Любые ШС могут входить не более чем в один раздел.

Если ШС не входит в состав раздела, возможно непосредственное управление его режимом (взятие на охрану и снятие с охраны). Если ШС включен в какой-либо раздел, управление режимом ШС возможно только в составе раздела.

Для индикации состояний разделов может использоваться световая и звуковая индикация считывателей.

Возможна настройка любого выхода контроллера для работы с исполнительными устройствами охранной подсистемы (сирена, ПЦН, световой оповещатель).

### 5.10.2 Настройка охранных функций без использования разделов

Управление режимом охраны автономно используемого входа возможно как внешнее (командой, передаваемой с ПК), так и внутреннее (через аппаратные взаимодействия – в качестве реакции на какое-либо событие). Для реализации локального управления, осуществляемого пользователями с использованием считывателей СКУД, необходимо настроить реакции на события считывателя «Постановка на охрану», «Снятие с охраны» либо на события «Ввод PIN 1..16 + PROX», «Ввод PIN 1 .. 16», а также настроить полномочия пользователей по управлению режимами охраны. Считыватель должен иметь дополнительную кнопку управления охраной либо иметь встроенную клавиатуру.

Для дверей не предусмотрено управление режимами охраны при использовании их вне раздела.

### 5.10.3 Настройка охранных функций с использованием разделов

Для добавления раздела в конфигурацию необходимо в дереве конфигурации из контекстного меню узла **«Разделы»** выбрать команду **«Добавить»**, а затем выбрать пункт **«Раздел»** (рисунок 68).

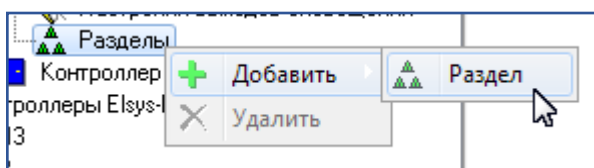



Рисунок 68 – Добавление раздела


В каждом контроллере Elsys-MB может быть создано до 8 разделов.

В раздел могут быть включены входы с типом ШС **«Охранный»**, **«Входной»**, **«Круглосуточный»** и **«Объем»**, имеющие номер в диапазоне 1..15.

Рекомендуется создавать отдельные разделы для каждого охраняемого помещения.

Окно свойств раздела содержит параметры настройки и списки устройств, для настройки состава раздела (рисунок 69).

Чтобы добавить устройство в раздел, необходимо выделить его в списке «Не входят в раздел» и нажать кнопку .

Чтобы исключить устройство из раздела, следует выбрать его в списке «Входят в раздел» и нажать кнопку .

«**Наименование раздела**» – наименование раздела, которое можно изменить в целях более удобного представления информации.

Группа параметров «**Управление разделом со считывателей**» доступна при наличии считывателей и позволяет для указанных в списке «**Считыватели, с которых разрешено управление**» считывателей разрешить локальное управление режимами охраны.

Локальное управление возможно одним из четырёх способов, описание которых дано в таблице 9.

Рисунок 69 – Свойства раздела

Таблица 9 – Способы управления режимами охраны с помощью считывателей

№	Способ управления режимом охраны	Описание
1	PIN-код + карта	<p>Постановка/снятие любого раздела возможны с любого считывателя (в пределах контроллера). Для управления режимом охраны необходимо ввести соответствующий PIN-код и предъявить карту.</p> <p>Для использования этого способа в настройках раздела должна быть включена опция <b>«PIN-код + карта»</b>. Этот способ нельзя использовать одновременно со способом <b>«только PIN-код»</b>. Считыватель должен быть оборудован клавиатурой. Должны быть заданы настройки <b>«PIN-код для постановки на охрану»</b> и <b>«PIN-код для снятия с охраны»</b>. Числовые значения этих паролей должны находиться в диапазоне 1 – 9999 и не должны совпадать ни с одним из служебных или пользовательских PIN-кодов.</p>
2	PIN-код	<p>Постановка/снятие любого раздела возможны с любого считывателя (в пределах контроллера).</p> <p>Для использования этого способа должна быть включена опция <b>«Только PIN-код»</b>. Этот способ нельзя использовать одновременно со способом <b>«PIN-код + карта»</b>. Считыватель должен быть оборудован клавиатурой. Должны быть заданы настройки <b>«PIN-код для постановки на охрану»</b> и <b>«PIN-код для снятия с охраны»</b>. Числовые значения этих паролей должны находиться в диапазоне 1 – 9999 и не должны совпадать ни с одним из служебных или пользовательских PIN-кодов. Поскольку при этом способе не используется карта доступа, использовать его следует в исключительных случаях.</p>
3	Кнопка + карта	<p>Для использования этого способа у раздела должна быть включена опция <b>«Кнопка и карта/ Удержание ключа»</b>.</p> <p>Кроме того, у считывателя, с которого предполагается выполнять управление режимами охраны, должна быть настроена кнопка управления режимом охраны, и должен быть назначен <b>«Раздел для управления и мониторинга»</b>.</p> <p>Для управления режимом охраны необходимо нажать кнопку и, удерживая её, предъявить карту. Раздел, если был на охране, будет снят с охраны, а если был вне охраны – будет взят на охрану.</p>
4	Удержание ключа	<p>Этот способ возможен, если считыватель подключен по интерфейсу 1-Wire (Touch Memory).</p> <p>Для использования этого способа у раздела должна быть включена опция <b>«Кнопка и карта/ Удержание ключа»</b>.</p> <p>Кроме того, у считывателя должна быть включена опция</p>

Таблица 9 – Способы управления режимами охраны с помощью считывателей

№	Способ управления режимом охраны	Описание
		<p><b>«Анализировать удержание ключа/карты»</b>, и должен быть назначен <b>«Раздел для управления и мониторинга»</b>. Для управления режимом охраны необходимо поднести к считывателю карту или ключ на время более 2 с. Раздел, если был на охране, будет снят с охраны, а если был вне охраны – будет взят на охрану. Если ключ поднести к считывателю на время менее 2 с, выполнится предоставление доступа.</p>

При использовании всех способов локального управления, кроме способа **«PIN-код»**, анализируются полномочия сотрудников **«Право постановки на охрану»** и **«Право снятия с охраны»** и обеспечивается авторизация действий по управлению режимами охраны.

Если соответствующее действие разрешено, при постановке (снятии) с охраны будет сформировано событие типа «Дверь...->Постановка (снятие) на охрану (с охраны) выходным (входным) считывателем» (с данными о пользователе, выполнявшем действие). Также будут сформированы события, отображающие изменение состояния раздела и входящих в его состав ШС.

**«Разрешить управление с ПК»** - опция позволяет включать (выключать) возможность управления разделом с компьютера с помощью команд, передаваемых по сетевому интерфейсу (RS-485 или Ethernet).

**«Досрочная постановка на охрану после выхода»** - опция позволяет включать (выключать) возможность досрочной постановки на охрану ШС, имеющих задержку взятия. При включенной опции, если после регистрации штатного выхода и закрытия двери, входящей в состав раздела, прошло 5 и более секунд, и все ШС, имеющие задержку взятия, перешли в состояние «Задержка взятия - готовность», все эти ШС будут досрочно поставлены на охрану.

**«Автоматическое снятие с охраны при входе в помещение»** - опция обеспечивает автоматическое снятие раздела с охраны при штатном входе в помещение. Для работы этой функции дверь, через которую осуществляется вход, должна входить в состав раздела, а сотрудник, осуществляющий вход, должен иметь полномочия «Снятие с охраны». Если таких полномочий нет, то при включенной настройке **«Автоматическое снятие с охраны при входе в помещение»** в доступе будет отказано с формированием сообщения «Отказ в доступе на вход – ограничение прав».

**«Протоколировать события»** - опция позволяет включать (выключать) регистрацию контроллером событий раздела.

**«Ставить на охрану, если все зоны готовы»** - опция задаёт логику работы раздела при постановке его на охрану. При попытке постановки раздела на охрану анализируется состояние ШС, входящих в его состав. Если эта опция включена, необходимым условием для постановки раздела на охрану является готовность к постановке на охрану всех ШС и



дверей, входящих в его состав. При выполнении этого условия выполняется постановка раздела на охрану и регистрируется событие «Раздел ХХ->На охране», а также события об изменении состояния ШС («Вход YY-> На охране» ..., «Дверь NN->На охране...»). Если хотя бы один ШС не готов к постановке на охрану, формируется событие «Раздел ХХ->Невзятие», и ни один из ШС, входящих в состав раздела, на охрану не ставится.

Если опция **«Ставить на охрану, если все зоны готовы»** выключена, раздел будет поставлен на охрану, если для каждого ШС, находящегося в нарушенном состоянии, выполняется хотя бы одно из условий:

- **«Задержка взятия на охрану»** не равна нулю;
- ШС имеет тип **«Объём»**, при наличии в разделе ШС типа **«Входной»** с ненулевой задержкой взятия (задержка взятия для ШС типа **«Объём»** равна максимальной задержке взятия среди ШС типа **«Входной»**, входящих в раздел);
- включена опция **«Автоматическое взятие после невзятия»**.

Если эти условия не выполняются хотя бы для одного из ШС, формируется событие «Раздел ХХ->Невзятие», и ни один из ШС, входящих в состав раздела, на охрану не ставится.

При успешной постановке раздела на охрану будет зарегистрировано событие «Раздел ХХ->На охране», а также события об изменении состояний ШС, входящих в раздел.

Для ШС, не имеющих задержки взятия на охрану и находящихся в физическом состоянии «Норма», будут зарегистрированы события вида «Вход YY-> На охране».

Для ШС, имеющих задержку взятия, и находящихся в состоянии «Норма», будут зарегистрированы события вида «Вход YY->Взятие на охрану с задержкой». Если же такой ШС находится в состоянии «Нарушено», будет сформировано событие «Вход YY->Задержка взятия – неготовность».

Для ШС, находящегося в состоянии **«Нарушено»** и имеющего включенную настройку **«Автоматическая постановка на охрану из состояния «Не взято»**, будет зарегистрировано событие «Невзятие».

По окончании времени задержки взятия на охрану соответствующие ШС, в зависимости от их физического состояния, перейдут либо в состояние **«На охране»**, либо в состояние **«Тревога»**.

ШС, имеющие настройку **«Автоматическая постановка на охрану из состояния «Не взято»**, будут находиться в состоянии «Невзятие» до тех пор, пока не восстановится нормальное состояние ШС. Если нормальное состояние ШС сохранится более 3 с, он перейдёт в состояние «На охране».

Любое нарушение ШС, находящегося в режиме «На охране», вызовет переход его в состояние «Тревога» либо «Тревога входной зоны». Для снятия тревоги потребуется снять раздел с охраны.



ШС типа **«Объём»** участвуют в работе раздела следующим образом. Задержка взятия на охрану для этих ШС принимается равной максимальной задержке взятия среди ШС типа **«Входной»**, входящих в раздел. Задержка тревоги принимается также равной максимальной задержке тревоги среди ШС типа **«Входной»**. Если ШС типа **«Объём»** в составе находящегося на охране раздела будет нарушен в момент пребывания ШС типа **«Входной»** в состоянии «Задержка тревоги», он также перейдёт в состояние «Задержка тревоги». В иных случаях ШС типа **«Объём»** немедленно перейдёт в состояние «Тревога».

При участии двери в составе раздела её датчик прохода используется в подсистеме доступа для регистрации прохода, а в охранной подсистеме – в качестве охранного датчика. При этом, учитывается не только физическое состояние датчика прохода, но и логическое состояние двери («открыто», «закрыто», «заблокировано», «разблокировано», «нормальный режим»). Дверь считается готовой к постановке на охрану, если она находится в нормальном режиме и в состоянии «Закрыто». Кроме того, при участии двери в составе раздела возможно использование событий СКУД (штатный вход или штатный выход) для управления режимами охранной подсистемы. Режим доступа двери также зависит от состояния раздела. Если раздел на охране, доступ в дверь, входящую в раздел, разрешён только сотрудникам с полномочиями «Право снятия с охраны».

Настройка **«Автоматическая постановка на охрану при выходе последнего сотрудника»** подробно описана в п. 9.3.

#### 5.10.4 Настройка световой и звуковой индикации состояний разделов

Встроенная световая и звуковая индикация считывателей СКУД может быть использована не только для индикации событий и состояний СКУД, но и для индикации состояния выбранного раздела и индикации действий пользователей по управлению охраной.

Для того, чтобы реализовать индикацию состояний и событий раздела на считывателе СКУД, следует выполнить следующие настройки (см. настройку считывателя):

- настроить для считывателя режим индикации **«События СКУД и состояние раздела»**;
- назначить раздел для управления и индикации;
- настроить для считывателя выходы управления красным светодиодом, зелёным светодиодом и звуком;
- установить требуемое значение для настройки считывателя **«Индицировать неготовность зон к постановке на охрану»**. Обычно для выходных (внутренних) считывателей эту настройку следует включать, а для входных – выключать.

Подробно алгоритмы индикации считывателей описаны в руководстве по эксплуатации СКУД Elsys.

#### 5.10.5 Настройка исполнительных устройств охранной подсистемы

В каждом контроллере Elsys-MB может быть запрограммировано до восьми исполнительных устройств охранной подсистемы.

Для настройки исполнительных устройств необходимо выбрать узел «Настройки выходов оповещения» (рисунок 70) и для требуемых выходов оповещений (ВО1..ВО8) установить параметры в соответствующих столбцах.

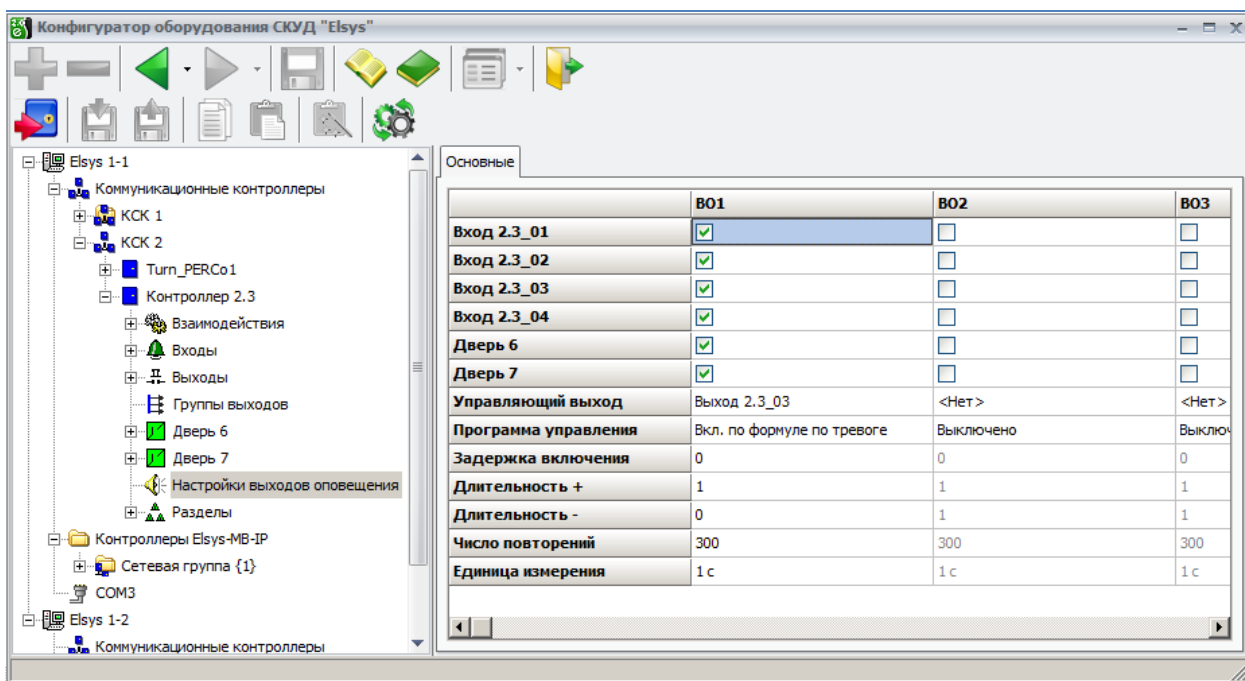


Рисунок 70 – Настройка выходов оповещения

Для управления исполнительными устройствами может быть назначен любой выход или группа выходов, которые задаются параметром **«Управляющий выход»**.

Для каждого исполнительного устройства должна быть задана **«Программа управления»**, в соответствии с которой управляющий выход будет реагировать на состояния связанных с ним ШС.

Если для выхода или группы выходов назначена функция управления устройством оповещения, управление им из управляющего ПО или через взаимодействия становится недоступным. Режим работы такого выхода полностью определяется логическим состоянием входов и дверей, связанных с ним, и программой управления.

Настройки устройств оповещения описаны ниже.

**«Управляющий выход»** - выход (или группа выходов), назначенный для управления исполнительным устройством.

**«ШС, связанные с управляющим выходом»** - входы, состояние которых анализируется при управлении исполнительным устройством.

**«Двери, связанные с управляющим выходом»** - двери, состояние которых анализируется при управлении исполнительным устройством.

**«Программа управления»** - алгоритм работы управляющего выхода. Возможно задание одной из программ управления:

- «Нет управления» (программа № 0);
- «Лампа» (программа № 1);
- «ПЦН» (программа № 2);
- «Включить по тревоге» (программа № 3);
- «Включить по формуле по тревоге» (программа № 4);
- «Пожарная лампа» (программа № 5).

Для программы управления актуальны настройки:

- «Задержка включения» (0 – 98 с);
- «Длительность положительной части периода» (0 – 98 с);
- «Длительность отрицательной части периода» (0 – 98 с);
- «Число повторений» (1 – 65534, 65535 – бесконечное время управления);
- «Единица измерения» (возможные значения – «0,1 с», «1 с», «10 с», «1 мин», «10 мин»).

В таблице 10 приведено описание программ управления исполнительными устройствами.

**Таблица 10 – Описание программ управления исполнительными устройствами**

№	Наименование программы управления	Описание работы
1	Лампа	<p>Программа, предназначенная для управления световым оповещателем.</p> <p>Если хотя бы один из связанных ШС находится в состоянии «Тревога», «Задержка тревоги», «Задержка взятия – неготовность», «Невзятие», управляющий выход пульсирует с частотой 1 Гц (0,5 с включено, 0,5 с выключено).</p> <p>Если хотя бы один из связанных ШС находится в состоянии «На охране» или «Задержка взятия – готовность», и нет ни одного связанного ШС, находящихся в одном из состояний «Тревога», «Задержка тревоги», «Задержка взятия – неготовность», «Невзятие», управляющий выход находится в состоянии «Включено».</p> <p>Если все ШС сняты с охраны (т. е. находятся в одном из состояний – «Неготовность» или «Норма - готовность»), управляющий выход находится в состоянии «Выключено».</p>
2	ПЦН	<p>Программа, предназначенная для выдачи сигнала на пульт централизованного наблюдения.</p> <p>Если все связанные ШС находятся в состоянии «На охране»,</p>

Таблица 10 – Описание программ управления исполнительными устройствами

№	Наименование программы управления	Описание работы
		управляющий выход находится в состоянии «Включено», иначе – в состоянии «Выключено».
3	Включить, если тревога	Если хотя бы один из связанных ШС находится в состоянии «Тревога», управляющий выход находится в состоянии «Включено», иначе – в состоянии «Выключено».
4	Включить по формуле, если тревога	Если хотя бы один из связанных ШС перешёл в состояние «Тревога», управляющий выход начинает работать по программе, задаваемой параметрами <b>«Задержка включения»</b> , <b>«Длительность положительной части периода»</b> , <b>«Длительность отрицательной части периода»</b> , <b>«Число повторений»</b> , <b>«Единица измерения»</b> . Если ни один из связанных ШС не находится в состоянии «Тревога», управляющий выход находится в состоянии «Выключено».
5	Пожарная лампа	Программа, предназначенная для управления световым оповещателем. Если хотя бы один из связанных ШС находится в состоянии «Тревога», «Задержка тревоги», «Задержка взятия – неготовность», «Невзятие», управляющий выход пульсирует с частотой 1 Гц (0,5 с включено, 0,5 с выключено). Если все связанные ШС находятся в состоянии «На охране», управляющий выход находится в состоянии «Включено». Если хотя бы один ШС снят с охраны, управляющий выход находится в состоянии «Выключено».

## 5.11 Настройка выходов и групп выходов

### 5.11.1 Настройка выходов

Для добавления выхода необходимо выбрать узел **«Выходы»** и вызвать контекстное меню, в котором нужно выбрать пункт **«Добавить»**, затем выбрать пункт **«Выход»** (рисунок 71)

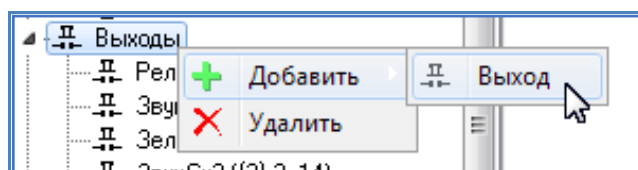


Рисунок 71 - Контекстное меню добавления выхода

Добавится выход с первым свободным номером. В правой части окна конфигуратора появится окно параметров выхода (рисунок 72).

Номер выхода определяет его физическое расположение на плате контроллера и его тип (1 – 4 – релейные, 5 – 18 – типа «открытый коллектор»).

Опция **«Инверсия»** позволяет выбрать режим работы выхода (если включена – нормально замкнутый, если выключена – нормально разомкнутый).

**«Мониторинг состояния выхода»** – при включенной опции контроллер регистрирует в протоколе сообщения об изменениях состояния выхода.

Основные Управление

Наименование устройства:  
Выход {2}.2\_02

Номер выхода:  
2 (Релейный выход)

Инверсия

Мониторинг состояния выхода

Мониторинг окончания работы выхода

Для команды "Импульс" использовать формулу

Задержка	0
+ полупериод	1
- полупериод	0
Число повторений	1
Единица измерения	1 с

Рисунок 72 - Окно параметров выхода

**«Мониторинг окончания работы выхода»** – при включенной опции контроллер регистрирует в протоколе сообщение об окончании работы по формуле.

Группа настроек **«Для команды «Импульс» использовать формулу»** позволяет задать алгоритм управления выходом, который будет выполняться при выполнении команды **«Импульс»** из ПО «Бастион-2». Данная группа настроек действительна только при запущенном ПО «Бастион-2» и не передается в контроллеры в процессе инициализации.

Если выход используется в конфигурации двери, турникета или считывателя, обычно используются настройки по умолчанию.

Вкладка **«Управление»** позволяет управлять выходом непосредственно из окна конфигуратора, (более подробно см. п. 5.16).

### 5.11.2 Настройка групп выходов

Группа выходов является логическим объединением нескольких выходов для одновременного обращения к ним как к обычному выходу. Группа выходов может быть пустой. Для каждого контроллера может быть создано до 12 групп выходов. Любые выходы могут входить в состав любых групп, в том числе нескольких.

Для добавления входа необходимо выбрать узел **«Группы выходов»** и вызвать контекстное меню, в котором выбрать пункт **«Добавить»**, а затем выбрать пункт **«Группу выходов»** (рисунок 73).

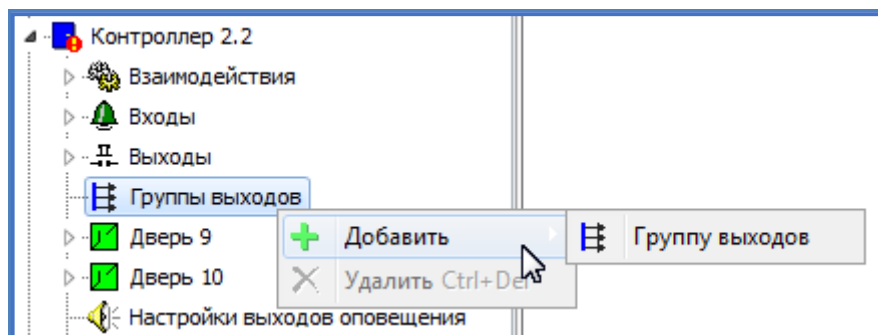




Рисунок 73 - Контекстное меню добавления группы выходов

Настройка основных свойств групп выходов аналогична настройке выходов (рисунок 72), за исключением того, что группа не может быть инверсной.

Закладка **«Состав группы»** (рисунок 74) позволяет включить в группу нужный набор выходов.

В левой части окна находится список выходов, не включённых в группу, а в правой части – список выходов, включённых в группу.

Добавление выхода в группу осуществляется выбором соответствующего выхода и нажатием на кнопку  или двойным щелчком левой кнопки мыши на соответствующем выходе в колонке **«Доступные выходы»**.

Удаление выхода из группы осуществляется выбором соответствующего выхода и нажатием на кнопку  или двойным щелчком левой кнопки мыши на соответствующем выходе в колонке **«Выбранные выходы»**.

Вкладка **«Управление»** позволяет управлять группой выходов непосредственно из окна конфигуратора (более подробно см. п. 5.16).

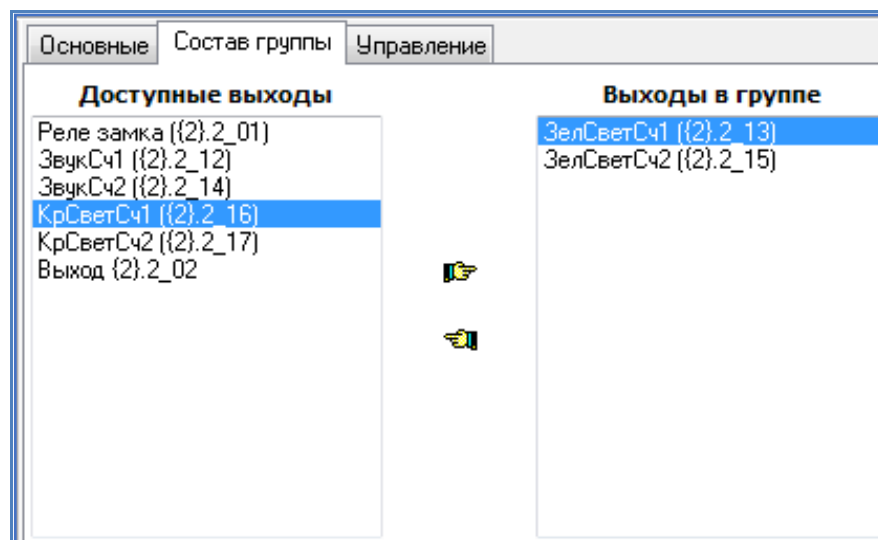


Рисунок 74 - Окно настройки состава группы выходов

## 5.12 Настройка считывателей

Окно свойств считывателя содержит пять вкладок: «Основные», «Дополнительные», «Доступ по нескольким картам», «Управление» и «Биометрический считыватель» (отображается при использовании биометрического считывателя).

### 5.12.1 Вкладка «Основные»

Основные параметры считывателя показаны на рисунке 75.

**«Номер считывателя»** – числовое значение, определяющее физическое расположение клеммных соединителей на плате контроллера, к которым подключается считыватель.

**«Имя устройства»** – текстовый идентификатор считывателя. По умолчанию содержит в составе текста часть, обозначающую точку доступа, к которой относится этот считыватель. Следует помнить, что именно имя считывателя (а не точек доступа) используется при настройке уровней доступа в программном обеспечении бюро пропусков.

**«Роль считывателя»** - эта настройка имеет два значения – **«Входной»** или **«Выходной»**.

**«Использовать устройства»** - возможны четыре варианта использования устройств идентификации: считыватель карт, считыватель карт и клавиатура, только клавиатура и биометрический считыватель. Настройка должна быть установлена в соответствии с реально установленным и используемым оборудованием. Набор входов и выходов, используемых считывателями и/или клавиатурами, зависит от настроек контроллера **«Тип клавиатур»** и **«Интерфейс считывателя»** (рисунок 36), а также варианта исполнения контроллера.

Группа настроек **«Полномочия дежурного оператора»** задаёт категории пользователей системы, доступ которым может быть предоставлен дежурным оператором нажатием кнопки «Подтверждение доступа» (при этом регистрируется соответствующее событие).



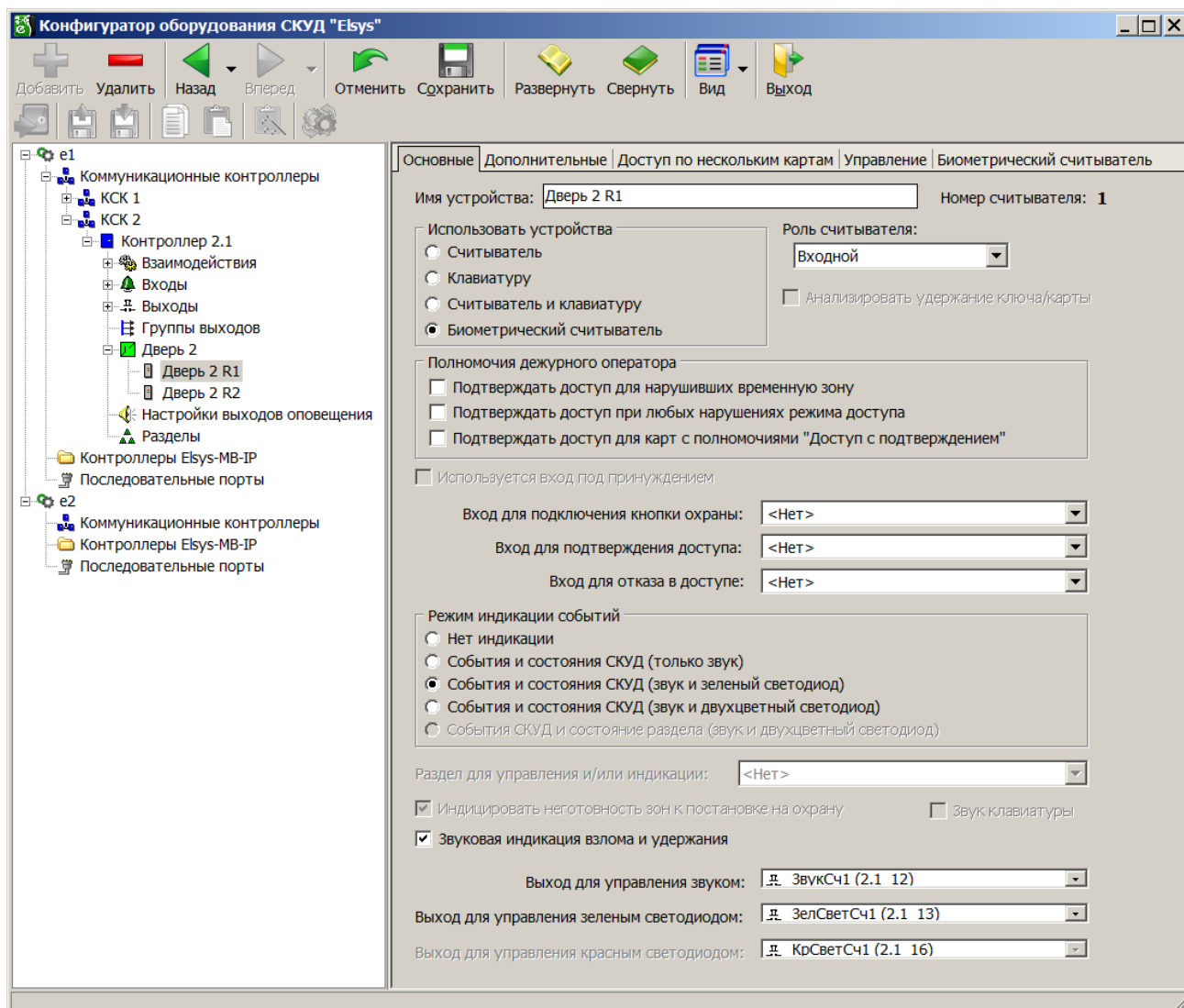


Рисунок 75 - Настройка основных параметров считывателя

«**Подтверждать доступ для нарушивших временную зону**» - опция включает (отключает) полномочия дежурного оператора подтверждать доступ для пользователей, нарушивших временную зону.

«**Подтверждать доступ при любых нарушениях режима доступа**» - опция включает (отключает) полномочия дежурного оператора подтверждать доступ для пользователей, нарушивших временную зону и(или) последовательность прохода.

«**Подтверждать доступ для пользователей с полномочиями «Доступ с подтверждением»**» - опция включает (выключает) полномочия дежурного оператора подтверждать доступ для пользователей, у которых пропуск с полномочием «Доступ с подтверждением».

«**Используется вход под принуждением**» - если эта опция включена, то при наличии клавиатуры становится возможным использовать режим «**Доступ под принуждением**». Если используется этот режим, пользователь системы может набрать «принудительный» PIN-код, предъявить карту и получить право доступа, точно также как и при штатном предъявлении карты, но при этом сформируются события «Предоставление доступа под принуждением», затем «Вход/выход под принуждением», являющиеся тревожными



сообщениями для дежурного оператора. «Принудительный» PIN-код отличается от штатного младшей цифрой, которая вычисляется следующим образом: если младшая цифра PIN-кода в диапазоне 0 - 4, необходимо прибавить число 5, если младшая цифра в диапазоне 5 - 9, необходимо отнять число 5. При использовании доступа под принуждением необходимо проследить, чтобы ни один «принудительный» код не совпадал с штатным PIN-кодом. Примерный рекомендуемый ряд PIN-кодов: 1..4, 15..24, 35..44 (при этом принудительными будут коды 6..14, 25..34) и т. д .

**«Вход для подключения кнопки охраны»** – вход для подключения кнопки, используемой для управления режимами охраны. Для этого входа должна быть установлена должным образом (как правило, нормально разомкнутый с временем интегрирования 70 мс) группа опций **«Тип входа»** на вкладке «Основные» в свойствах входа (п. 5.9.1, рисунок 67). При нажатой кнопке одно- и двукратное предъявление карты соответствующему считывателю интерпретируется как события «Постановка на охрану» и «Снятие с охраны» соответственно. Для использования этих событий необходимо настроить взаимодействия.

**«Вход для подтверждения доступа»** и **«Вход для отказа в доступе»** – входы контроллера, используемые для подключения кнопок подтверждения или отказа в доступе. Если точка доступа двусторонняя, то для входного и выходного считывателя эти настройки могут совпадать. Для этих входов должна быть установлена должным образом (как правило, нормально разомкнутый с временем интегрирования 70 мс) группа опций «Тип входа» на вкладке «Основные» свойств входа (п. 5.9.1, рисунок 67)

**«Режим индикации событий»** –настройка, позволяющая назначить выходы управления индикацией: **«Выход управления зелёным светодиодом»**, **«Выход управления красным светодиодом»**, **«Выход управления звуком»**, в зависимости от используемого алгоритма индикации.

В качестве выходов управления индикацией могут быть назначены любые выходы или группы выходов.

Настройка **«Режим индикации событий»** может принимать одно из пяти возможных значений. В таблице 11 кратко описаны все возможные алгоритмы индикации.

**Таблица 11 - Описание режимов индикации считывателей**

Режим № 0	«Индикация отсутствует»
Встроенная индикация отсутствует. При необходимости индикация может быть организована настройкой взаимодействий.	
Режим № 1	«События и состояния СКУД (только звук)»
Режим индикации, обеспечивающий звуковую индикацию событий СКУД. Для считывателя необходимо назначить <b>«Выход управления звуком»</b> . Включение этого режима эквивалентно включению настройки <b>«Звук считывателя»</b> , использовавшейся в версиях контроллера Elsys-MB ниже 2.60.	

Таблица 11 - Описание режимов индикации считывателей

Для использования в этом режиме светодиодной индикации необходимо настроить взаимодействия.	
<b>Режим № 2</b>	<b>«События и состояния СКУД (звук и зелёный светодиод)»</b>
<p>Режим индикации, обеспечивающий звуковую индикацию событий СКУД, а также индикацию событий и состояний СКУД зелёным светодиодом.</p> <p>Также обеспечивается световая и звуковая индикация действий по управлению режимами охраны.</p> <p>Обеспечивается индикация следующих режимов точки доступа:</p> <ul style="list-style-type: none"> <li>• нормальный режим;</li> <li>• открыто/разблокировано;</li> <li>• звук при взломе/удержании;</li> <li>• ожидание подтверждения.</li> </ul> <p>В этом режиме предполагается использование красного светодиода считывателя как индикатора питания.</p> <p>В считывателе должен быть выбран режим, при котором при включении зелёного светодиода красный светодиод должен гаснуть. Если это невозможно, красный светодиод должен быть выключен.</p>	
<b>Режим № 3</b>	<b>«События и состояния СКУД (звук и двухцветный светодиод)»</b>
<p>Режим индикации, обеспечивающий звуковую индикацию событий СКУД, а также индикацию событий и состояний СКУД двухцветным светодиодом.</p> <p>Обеспечивается индикация следующих режимов точки доступа:</p> <ul style="list-style-type: none"> <li>• нормальный режим;</li> <li>• открыто/разблокировано;</li> <li>• взлом со звуком или без;</li> <li>• удержание со звуком или без;</li> <li>• заблокировано;</li> <li>• ожидание подтверждения.</li> </ul> <p>Также обеспечивается световая и звуковая индикация действий по управлению режимами охраны.</p>	
<b>Режим № 4</b>	<b>«События СКУД и состояние раздела (звук и двухцветный светодиод)»</b>
<p>Управление звуком и двухцветным светодиодом. Индицируются события СКУД и состояния назначенного охранного раздела (состояния – на охране, задержка взятия – готовность, задержка взятия - неготовность, задержка тревоги, тревога, вне охраны, готовность, неготовность объёмного ШС, неготовность периметрального ШС, неготовность входного ШС, открыта/разблокирована дверь в разделе).</p>	
<p><b>Примечание.</b> Для реализации режимов 3, 4 считыватель должен обеспечивать свечение индикатора жёлтым цветом при одновременном управлении включением красного и зелёного</p>	

**Таблица 11 - Описание режимов индикации считывателей**

светодиодов. Информацию об особенностях индикации считывателя следует искать в его техническом описании.

Настройка **«Раздел для управления и/или индикации»** назначает раздел, состояние которого будет индицироваться светодиодами и звуковым сигнализатором считывателя в режиме индикации 4. Кроме того, назначенным разделом можно управлять, используя кнопку управления охраной или удерживая карту.

Настройка **«Анализировать удержание ключа/карты»** действует только в случае, если считыватель подключен по интерфейсу Touch Memory. Если назначен раздел для управления и индикации, удерживание ключа свыше 2 с вызовет снятие раздела с охраны (если раздел был на охране), либо постановку раздела на охрану (если он был снят с охраны).

Настройка **«Индицировать неготовность зон к постановке на охрану»** актуальна при использовании режима индикации 4. Если включена эта настройка, при неготовности ШС светодиодный индикатор будет отображать жёлтым цветом (мигающим или постоянно светящимся – в зависимости от типа ШС, находящихся в состоянии «Неготовность») неготовность ШС.

Настройка **«Звуковая индикация взлома и удержания»** (актуальна для режимов индикации 1 – 3) обеспечивает звуковую индикацию состояний точки доступа «Взлом» и «Удержание».

**«Звук клавиатуры»** - если включена эта опция, то каждое нажатие на клавиатуре, относящейся к считывателю, сопровождается коротким звуковым сигналом на выходе для управления звуком этого считывателя.

Подробно режимы индикации считывателей описаны в документе «Руководство по эксплуатации СКУД Elsys».

### 5.12.2 Вкладка «Дополнительные»

Дополнительные настройки считывателей показаны на рисунке 76.

Группа настроек **«Мониторинг событий»** задаёт, какие события будут регистрироваться контроллером в протоколе событий и передаваться по интерфейсу RS-485.

Основные    Дополнительные    Доступ по нескольким картам    Управление

Мониторинг событий

- Мониторинг предоставления доступа
- Мониторинг событий "Действие 1", "Действие 2", "Действие 3"
- Мониторинг событий "Постановка на охрану", "Снятие с охраны", "Удержание ключа/карты"

Доступ при нарушениях режима

- Предоставлять доступ при нарушении временной зоны  
Допустимое опоздание: Любое
- Предоставлять доступ при нарушении зоны доступа

Игнорировать опцию пропуска "Доступ с подтверждением"

Интервал между набором кода и предъявлением карты, не более, с: 12

Интервал при предъявлении нескольких карт, не более, с: 12

Интервал при постановке на охрану, не более, с: 3

Интервал при предъявлении любых карт, не менее, с: 0

Рисунок 76 - Настройка дополнительных параметров считывателей

**«Мониторинг предоставления доступа»** - опция включает (отключает) мониторинг события «Предоставление доступа», во многих случаях данная опция может быть отключена, так как обычно за событием «Предоставление доступа» следует событие «Штатный проход».

**«Мониторинг событий «Постановка на охрану», «Снятие с охраны», «Удержание ключа/карты»** - опция включает (отключает) мониторинг событий по управлению охраной, обычно, эту опцию следует включать.

**«Мониторинг событий «Действие 1», «Действие 2» и «Действие 3»** - опция включает (отключает) мониторинг событий «Действие 1», «Действие 2», «Действие 3», которые формируются, если в дополнительных параметрах драйвера «Бастион-2 – Elsys» предъявляемого пропуска включены соответствующие опции.

**«Доступ при нарушениях режима»** - группа настроек, которые позволяют включать (отключать) «мягкие» режимы регистрации нарушений. В «мягком» режиме нарушение фиксируется, но доступ предоставляется.

При включенной опции **«Предоставлять доступ при нарушении временной зоны»** - при нарушении временной зоны сначала формируется событие «Нарушение временной зоны», а затем предоставляется доступ.

При регистрации нарушения временной зоны может быть задано максимально допустимое опоздание, то есть время после окончания разрешённого интервала, в течение которого будет разрешён доступ.

Опция **«Предоставлять доступ при нарушении зоны доступа»** относится к режиму антипассбэка. Если данная опция включена, то в режиме антипассбэка при нарушении зоны доступа сначала формируется событие «Нарушение зоны доступа», а затем предоставляется доступ.

Опция **«Игнорировать опцию пропуска «Доступ с подтверждением»** позволяет для отдельного считывателя не использовать дополнительный параметр пропуска **«Доступ с подтверждением»**.

**«Интервал между набором кода и предъявлением карты»** – интервал времени (1 – 127 с), отсчитываемый после ввода PIN-кода, используемый для ожидания предъявления карты. По окончании этого интервала введённый PIN-код сбрасывается.

**«Интервал при предъявлении нескольких карт»** – интервал времени между предъявлением двух карт (1 – 127 с) при осуществлении доступа по двум или трём картам.

**«Интервал при постановке на охрану»** – интервал времени (1 – 127 с), в течение которого ожидается повторное предъявление карты при управлении охраной. Если в течение этого времени карта не была предъявлена повторно, выполняется постановка на охрану, а если была предъявлена – выполняется снятие с охраны.

**«Интервал при предъявлении любых карт»** – время (0 – 127 с) с момента предъявления последней карты, в течение которого считыватель не реагирует на предъявление карт. Опция действует для контроллеров версии 2.47 и старше.

### 5.12.3 Вкладка **«Доступ по нескольким картам»**

На странице свойств **«Доступ по нескольким картам»** (рисунок 77) находятся настройки считывателей, используемые при настройке доступа по правилу двух (трёх) лиц.

Встроенный алгоритм доступа по правилу двух (трёх) лиц реализован в контроллерах версий 2.47 и старше.

Настройка **«Необходимое количество карт для получения доступа»** (возможные значения – 1, 2, 3) задаёт количество карт, которые необходимо предъявить для получения доступа.

Для каждой из последовательно предъявляемых карт могут быть заданы опции (см. п. 9.2), необходимые для получения доступа (возможные варианты – «Любая карта», «Действие 1», «Действие 2», «Действие 3»).

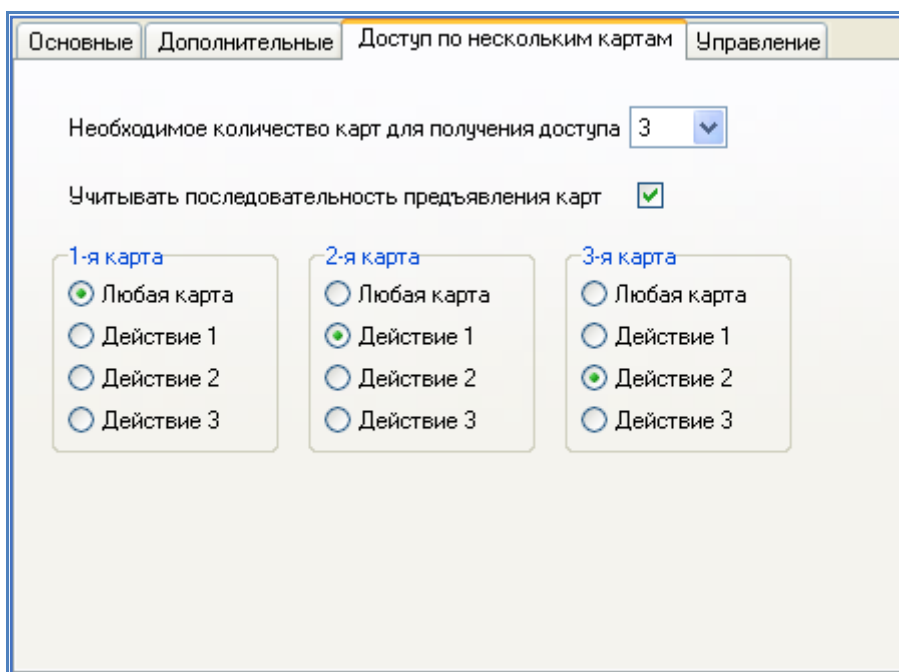


Рисунок 77 - Доступ по нескольким картам

Если включена настройка считывателя **«Учитывать последовательность предъявления карт»**, карты следует предъявлять в строго определённом порядке, в зависимости от необходимых опций. Если же эта настройка выключена, карты можно предъявлять в произвольном порядке.

В примере, показанном на рисунке 77, для получения доступа необходимо первой предъявить любую карту, имеющую право доступа, второй – карту с полномочиями «Действие 1», третьей – карту с полномочиями «Действие 2». Особенности настройки контроллеров Elsys-MB-SM

Контроллер Elsys-MB-SM является младшей, функционально упрощенной моделью в семействе контроллеров Elsys-MB, совместимой по протоколу и настройкам со старшими моделями. Контроллеры имеют значительно меньшее число настроек, а все входы и выходы имеют фиксированное назначение.

В конфигураторе драйвера «Бастион-2 – Elsys» у контроллеров Elsys-MB-SM отсутствуют узлы: **«Входы»**, **«Выходы»**, **«Группы выходов»**, **«Взаимодействия»**, **«Формулы выходов»**, **«Логические формулы»**, **«Служебные PIN-коды»**. Отсутствует возможность работы с турникетами и воротами. Для корректной работы контроллера необходимо добавить в соответствии с конфигурацией узлы **«Дверь»**, **«Считыватель»**, и выполнить их настройку.

#### 5.12.4 Вкладка «Биометрический считыватель»

Настройки биометрического считывателя показаны на рисунке 78.

**«Тип считывателя»** – тип подключенного к контроллеру биометрического считывателя. Доступны следующие типы: ЛКД КО-60 00, ЛКД КО-15 00, ЛКД КО-75 00, Elsys-PVR, EnterFace 3D, Suprema.

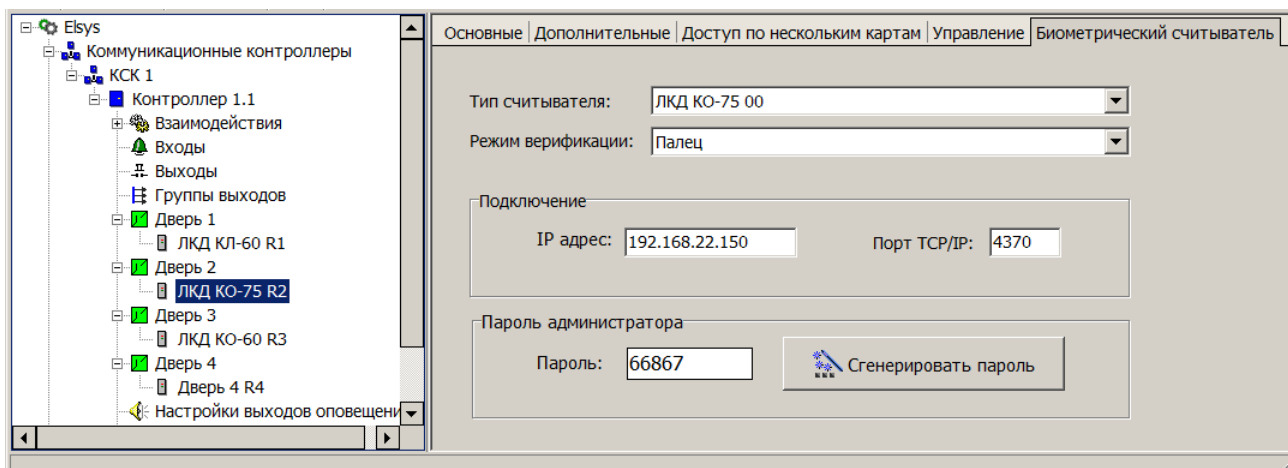


Рисунок 78 – Настройки биометрического считывателя

«Режим верификации» – задаёт совокупность признаков, которые будут использоваться для идентификации. Список возможных режимов верификации зависит от типа считывателя и приведён в таблице 12.

Таблица 12 – Режимы верификации биометрических считывателей

Тип считывателя	Режимы верификации
ЛКД КО-60 00	<ul style="list-style-type: none"> <li>Палец</li> <li>Палец и PIN-код PIN может иметь длину от 4 до 6 цифр. При длине PIN-кода в Бюро Пропусков более 6 цифр, в считыватель будут записаны только последние 6 цифр. Лидирующие нули вводить обязательно. PIN может полностью состоять из нулей</li> </ul>
ЛКД КО-15 00	<ul style="list-style-type: none"> <li>Карта</li> <li>Палец</li> <li>Палец или карта</li> <li>Палец и карта</li> </ul>
ЛКД КО-75 00	<ul style="list-style-type: none"> <li>Карта</li> <li>Палец</li> <li>Палец или карта</li> <li>Палец и карта</li> <li>Палец и PIN-код</li> <li>Карта и PIN-код</li> <li>Карта, PIN-код и палец PIN может иметь длину от 4 до 5 цифр. При длине PIN-кода в Бюро Пропусков более 5 цифр, в считыватель будут записаны только последние 5 цифр. Лидирующие нули вводить обязательно. PIN может полностью состоять из нулей</li> </ul>
Elsys-PVR	<ul style="list-style-type: none"> <li>Ладонь</li> </ul>

Таблица 12 – Режимы верификации биометрических считывателей

Тип считывателя	Режимы верификации
	<ul style="list-style-type: none"> <li>• (Карта или PIN-код) и ладонь (в этом режиме ладонь будет проверяться только у тех лиц, отпечаток ладони которых есть в БД.) PIN может иметь длину от 1 до 6 цифр. При длине PIN-кода в Бюро Пропусков более 6 цифр, в считыватель будут записаны только последние 6 цифр. Лидирующие не вводятся. PIN не может полностью состоять из нулей</li> </ul>
EnterFace 3D, EnterFace 3D Gate	<ul style="list-style-type: none"> <li>• Лицо</li> <li>• Карта и Лицо</li> </ul> <p>Режим верификации считывателей EnterFace 3D и EnterFace 3D Gate настраивается непосредственно в считывателе, через встроенный веб-интерфейс.</p>
Suprema	<ul style="list-style-type: none"> <li>• Карта</li> <li>• Палец</li> <li>• Карта и палец</li> <li>• Палец и PIN-код</li> <li>• Карта и PIN-код</li> <li>• Карта и PIN-код или палец</li> <li>• Карта, PIN-код и палец</li> </ul>

**«Интерфейс считывателя карт»** – настройка активна только для считывателей Elsys-PVR и EnterFace. Задаёт формат, в котором биометрический считыватель получает код карты со считывателя бесконтактных карт (при его наличии) и передаёт в контроллер Elsys при успешной идентификации пользователя. Возможные варианты:

- EnterFace - Wiegand-26, -33, -34, -37, -40, -42.
- Elsys-PVR - Wiegand-26, -42 (имеет встроенный считыватель бесконтактных карт)

При необходимости идентификации пользователя по карте и лицу, необходимо выбирать считыватель, имеющий один из вышеуказанных интерфейсов.

**При выборе считывателя с интерфейсом, отличным от Wiegand-26, следует проконсультироваться с разработчиком Бастион-Elsys, во избежание проблем с несовместимостью.**

**«IP адрес»** и **«Порт TCP/IP»** – параметры подключения к биометрическому считывателю. **«IP адрес»** должен быть установлен в соответствии с настройками в самом считывателе. Метод настройки IP адреса в считывателях различается:

- ЛКД-КО-15 - адрес настраивается через Ethernet с помощью программы «Search Panels and Modify IPAddress.exe», поставляемой производителем;
- ЛКД-КО-60 и ЛКД-КО-75 настраиваются через собственную клавиатуру и тачскрин;



- Elsys-PVR – через программу PVR Office;
- EnterFace настраиваются через веб-интерфейс;
- Suprema – либо через собственный тачскрин, либо с помощью ПО, поставляемое производителем считывателей. *Внимание:* поддерживается только шифрованная SSL-связь, поэтому не допускается отключение шифрования в считывателях.

**«Порт TCP/IP»:**

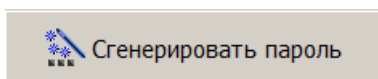
- для считывателей ЛКД следует установить равным 4370;
- для считывателей EnterFace следует установить равным 8085;
- для Elsys-PVR номер порта настраивается через ПО "PVR Office", по умолчанию имеет значение 5999;
- для Suprema номер порта устанавливается либо через собственный тачскрин, либо с помощью ПО, поставляемое производителем считывателей; по умолчанию имеет значение 51211.

**«Пароль»** - пароль администратора для считывателей ЛКД КО-60 00, ЛКД КО-75 00, Elsys-PVR, Suprema. Для считывателей ЛКД пароль генерируется автоматически при добавлении считывателя, но может быть изменен при необходимости.

При каждом восстановлении связи, а также при инициализации, в считыватели ЛКД КО-60 00, ЛКД КО-75 00 добавляется администратор с кодом «33554431» (0x1FFFFFFF) и вышеуказанным паролем, для исключения доступа обычных пользователей к настройкам считывателя через клавиатуру и тачпад.

Пароль администратора должен содержать только цифры, а его длина зависит от типа считывателя:

- для ЛКД КО-60 00 - длина пароля 6 знаков,
- для ЛКД КО-75 00 - длина пароля 5 знаков,



Кнопка генерирует новый пароль по псевдослучайному закону.

Для считывателя Elsys-PVR пароль должен соответствовать паролю, занесённому в считыватель с помощью ПО "PVR Office", по умолчанию имеет значение "root".

Для Suprema при каждой инициализации или очистке пользователей в считыватели добавляется администратор с ID=1 и заданным в конфигураторе паролем. По умолчанию пароль – «375422». Администратор не имеет возможности идентификации по карте или биометрическим данным.

## 5.13 Особенности настройки контроллеров Elsys-MB-SM

### 5.13.1 Настройка контроллеров

Для контроллеров Elsys-MB-SM актуальны следующие настройки (их назначение описано в п. 5.5):

- «Интерфейс считывателей»;
- «Разрешить локальный контроль последовательности прохода»;
- «Разрешить глобальный контроль последовательности прохода»;
- «Сброс в полночь»;
- «Тайм-аут для режима MULTIMASTER»;
- «Задержка ответной посылки»;
- «Автоматическая инициализация»;
- «Время инициализации».

Все остальные настройки в контроллерах Elsys-MB-SM не используются и в конфигураторе оборудования недоступны.

***Внимание!** Использование настройки глобального контроля последовательности прохода в контроллерах Elsys-MB-SM возможно, если в памяти контроллера не более 150 карт.*

### 5.13.2 Настройка дверей

Контроллер Elsys-MB-SM может обслуживать либо одну двустороннюю дверь, либо две двери с односторонним контролем доступа.

Для дверей, относящихся к контроллерам Elsys-MB-SM, используются следующие настройки (их назначение описано в п. 5.8):

- «Тип замка»;
- «Задержка включения выхода»;
- «Время включения выхода»;
- «Время шунтирования датчика прохода»;
- «Автозакрывание двери»;
- «Отслеживать фактический проход»;
- «Не регистрировать событие «Закрытие двери»;
- «Регистрировать событие «Взлом» как «Открывание»;
- «Регистрировать события «Блокировка», «Разблокировка», «Норма»;

- **«Единица измерения».**

Остальные настройки дверей не используются и в конфигураторе недоступны.

### 5.13.3 Настройка считывателей

Для считывателей, обслуживаемых контроллерами Elsys-MB-SM, используются следующие настройки (их назначение описано в п. 5.12):

- **«Роль считывателя»;**
- **«Использовать устройства»;**
- **«Мониторинг предоставления доступа»;**
- **«Предоставлять доступ при нарушении временной зоны»;**
- **« Предоставлять доступ при нарушении зоны доступа».**

Остальные настройки считывателей не используются и в конфигураторе недоступны.

## 5.14 Особенности настройки модулей Elsys-IO/MB

Модули Elsys-IO/MB, имеющие 16 выходов типа «открытый коллектор», совместимы по протоколу обмена с контроллерами Elsys-MB и работают в одной линии связи с ними под управлением драйвера «Бастион-2 – Elsys».

В конфигураторе драйвера «Бастион-2 – Elsys» у модулей «ElsysIO/MB» присутствуют только узлы **«Выходы»**, **«Взаимодействия»** и **«Формулы выходов»**. В базу данных может быть добавлено до 16 выходов, до 50 взаимодействий и до 16 формул выходов. Настройка выходов и формул управления выходами выполняется так же, как и для контроллеров Elsys-MB.

При настройке взаимодействий объектами управления могут быть выходы модуля, при этом доступны команды **«Включить»**, **«Выключить»**, **«Перебросить»**, **«Включить по формуле»**.

В качестве источников событий могут быть:

- контроллер (событие «Сброс»);
- другие контроллеры (события № 1 – 64, «Потеря/восстановление связи»);
- выходы самого модуля (события «Включение», «Выключение», «Окончание работы по формуле»).

## 5.15 Особенности настройки охранных контроллеров Elsys-MB-AC

### 5.15.1 Настройки контроллеров

Для контроллеров Elsys-MB-AC актуальны следующие настройки (их назначение описано в п. 5.5):

«Интерфейс считывателей»;

«Тайм-аут для режима MULTIMASTER»;

«Задержка ответной посылки»;

«Автоматическая инициализация»;

«Время инициализации».

Все остальные настройки в контроллерах Elsys-MB-AC не используются и в конфигураторе оборудования недоступны.

При добавлении контроллера Elsys-MB-AC в базу данных автоматически добавляются два виртуальных устройства – дверь и считыватель, которые невозможно удалить отдельно от прибора.

Устройство «Дверь», которому может быть задано любое удобное имя, в дальнейшем будет использоваться в качестве объекта-источника событий для действий по управлению режимами охраны.

Устройство «Считыватель» может быть использовано для задания настройки, **«Раздел для управления и/или индикации»** назначающей раздел, состояние которого будет индицироваться светодиодами и звуковым сигнализатором считывателя. Осуществлять управление в Elsys-MB-AC, в отличие от старших моделей контроллеров, можно любым разделом, в соответствии с полномочиями сотрудника.

Следует учитывать, что если считыватель, имеющий встроенную клавиатуру, подключен к контроллеру Elsys-MB-AC по интерфейсу Wiegand, то контроллер автоматически распознаёт коды нажатых клавиш. Идентификация пользователей осуществляется всегда в режиме «Только карта», а вводимый с клавиатуры PIN-код может быть использован в качестве параметра, выбирающего раздел для управления.

### 5.15.2 Настройка входов

Контроллеры Elsys-MB-AC имеют восемь аналоговых входов (№№ 1 – 8), которые могут быть использованы в качестве охранных входов, а также в качестве универсальных входов общего назначения.

Настройки входов контроллера Elsys-MB-AC полностью идентичны настройкам аналоговых входов контроллеров Elsys-MB-Pro, -Standard, -Light, -Pro4.

Аналоговые входы контроллера Elsys-MB-AC отличаются по электрическим характеристикам от аналоговых входов других контроллеров линейки Elsys-MB. Информация об этих отличиях приведена в руководстве по эксплуатации Elsys-MB-AC.

### 5.15.3 Настройка выходов

Контроллер Elsys-MB-AC имеет три выхода (O1 и O2 – релейные выходы, O3 – выход типа «Открытый коллектор»), каждый из которых может быть использован в качестве выхода оповещения либо как выход общего назначения.

Настройки «Инверсия», «Мониторинг состояния выхода», «Мониторинг окончания работы выхода» для выходов контроллера Elsys-MB-AC недоступны.

Выходы контроллера Elsys-MB-AC, управляющие линиями световой и звуковой индикации считывателя, имеют фиксированное назначение и не могут быть использованы в качестве выходов общего назначения.

### 5.15.4 Настройка охранных разделов

Охранные разделы контроллера Elsys-MB-AC настраиваются аналогично охранным разделам контроллеров доступа старшей линейки, с учётом имеющихся ограничений. Окно настройки разделов изображено на рисунке 79.

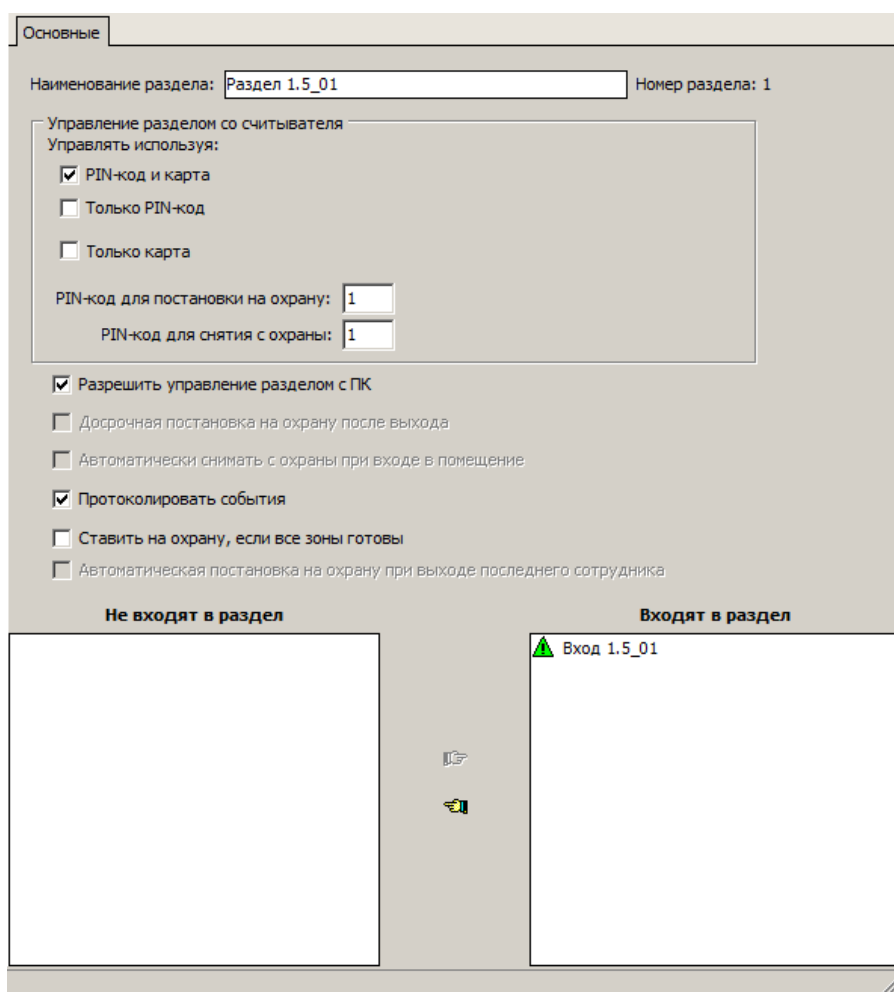


Рисунок 79 – Окно настройки охранного раздела контроллера Elsys-MB-AC

Настройки «Досрочная постановка на охрану», «Автоматически снимать с охраны при входе в помещение», «Автоматическая постановка на охрану при выходе последнего сотрудника» для контроллера Elsys-MB-AC недоступны, так как контроллер Elsys-MB-AC не осуществляет контроль и управление доступом.

Возможные способы управления режимами охраны с помощью считывателя контроллера Elsys-MB-AC описаны в таблице 13.

**Таблица 13 – Способы управления режимами охраны с помощью считывателей**

№	Способ управления режимом охраны	Описание
1	PIN-код + карта	<p>Для управления режимом охраны необходимо ввести соответствующий PIN-код и, после отображения на индикаторах считывателя состояния выбранного раздела, предъявить карту. Команда управления будет сформирована в соответствии с введённым PIN-кодом и полномочиями сотрудника.</p> <p>Для использования этого способа в настройках раздела должна быть включена опция <b>«PIN-код + карта»</b>. Этот способ нельзя использовать одновременно со способом <b>«только PIN-код»</b>. Считыватель должен быть оборудован клавиатурой. Должны быть заданы настройки <b>«PIN-код для постановки на охрану»</b> и <b>«PIN-код для снятия с охраны»</b> (эти PIN-коды могут совпадать).</p>
2	PIN-код	<p>Для использования этого способа должна быть включена опция <b>«Только PIN-код»</b>. Этот способ нельзя использовать одновременно со способом <b>«PIN-код + карта»</b>. Считыватель должен быть оборудован клавиатурой. Должны быть заданы настройки <b>«PIN-код для постановки на охрану»</b> и <b>«PIN-код для снятия с охраны»</b> (эти PIN-коды могут совпадать).</p>
3	Карта	<p>Для использования этого способа у раздела должна быть включена опция <b>«Только карта»</b>.</p> <p>Для управления режимом охраны необходимо предъявить карту, имеющую необходимые полномочия, после чего на индикаторах считывателя отобразится состояние выбранного раздела. Затем нужно повторно предъявить карту, после чего, раздел, если был на охране, будет снят с охраны, а если был вне охраны – будет взят на охрану.</p>

При использовании всех способов локального управления, кроме способа **«PIN-код»**, контроллер анализирует полномочия сотрудников и обеспечивает авторизацию действий по управлению режимами охраны.

Если соответствующее действие разрешено, при постановке (снятии) с охраны будет сформировано событие типа «Дверь...->Постановка (снятие) на охрану (с охраны) входным считывателем» (с данными о пользователе, выполнявшем действие). Также будут сформированы события, отображающие изменение состояния раздела и входящих в его состав ШС.

### 5.15.5 Настройка исполнительных устройств охранной подсистемы

Настройка исполнительных устройств контролера Elsys-MB-AC выполняется аналогично настройке исполнительных устройств контроллеров доступа старшей линейки (см. п. 5.10.5). Основные ограничения:

- число выходов – 3;
- адреса выходов жёстко закреплены за номерами устройств оповещения и соответствуют им (в качестве устройства оповещения № 1 может быть назначен только выход 1, в качестве устройства оповещения № 2 - только выход 2, в качестве устройства оповещения № 3 - только выход 3).

### 5.15.6 Группы управления охраной

Группы управления охраной (ГУО) позволяют настроить полномочия сотрудников по управлению охраной. Для настройки ГУО используется конфигуратор, который вызывается с помощью пункта «Группы управления охраной...» ленты управления «Операторы и полномочия» на вкладке «Конфигурация» главного меню ПО «Бастион-2» (рисунок 80).

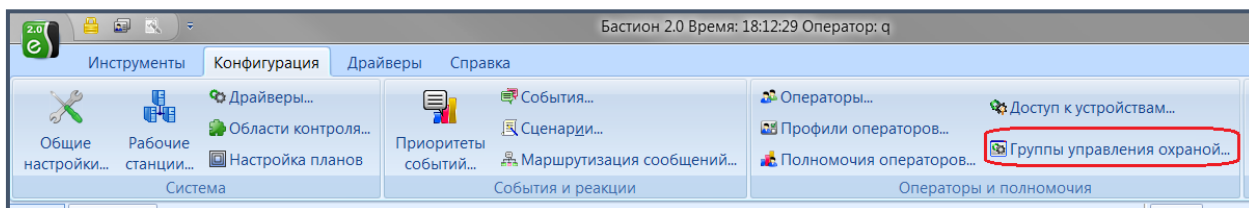


Рисунок 80 – Вызов окна конфигуратора ГУО

Подробное описание настройки ГУО приведено в документе «Руководство системного администратора».

Главное окно конфигуратора ГУО показано на рисунке 81.

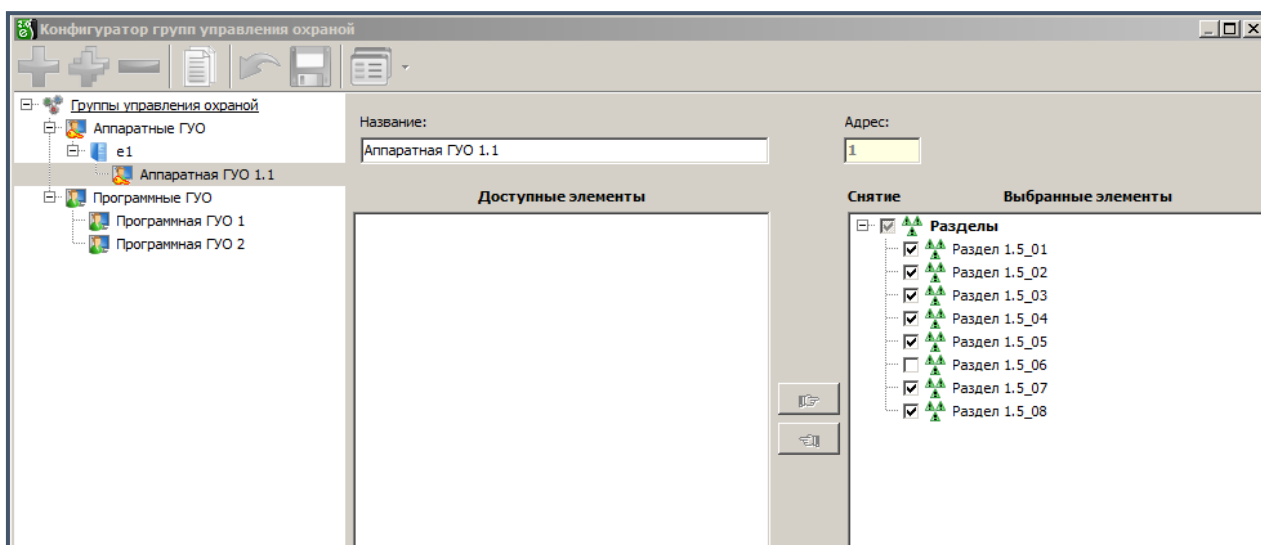


Рисунок 81 – Окно конфигуратора групп управления охраной

Для каждого экземпляра драйвера Elsys необходимо создать и настроить аппаратные ГУО. В аппаратные ГУО следует включать только разделы приборов Elsys-MB-AC, так как текущие версии контроллеров доступа старшей линейки не поддерживают работу с ГУО.

Следует учитывать, что разделами приборов Elsys-MB-AC можно управлять только со считывателя самого прибора. Если в группу управления охраной входят несколько разделов, то для управления будет выбран либо раздел с самым младшим адресом (если используется способ управления «Карта»), либо раздел, соответствующий введённому PIN-коду (если используется способ управления «PIN-код + карта»).

Если в системе присутствует несколько экземпляров драйверов СКУД Elsys, либо иные драйвера, использующие ГУО, и необходимо создать набор полномочий, охватывающий оборудование нескольких экземпляров драйверов, следует создать программную ГУО, состоящую из нескольких аппаратных ГУО.

Для назначения конкретному сотруднику заранее настроенных полномочий следует в Бюро пропусков на вкладке «Управление охраной» и назначить ему программную или аппаратную ГУО (Рисунок 82).

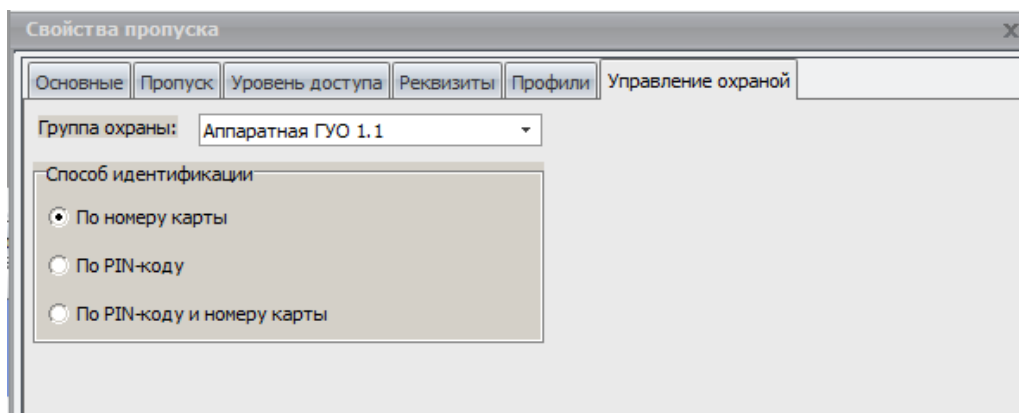


Рисунок 82 – Присвоение сотруднику группы управления охраной

**Внимание!** Следует помнить, что настройка «Способ идентификации», задаваемая конкретному сотруднику, не используется драйвером «Бастион-2 – Elsys». В СКУД Elsys, вне зависимости от значения этой настройки, используется способ идентификации «По номеру карты», а PIN-код для идентификации сотрудников не используется. Настройка «Способ идентификации» никак не связана со способом управления, задаваемым в настройках разделов контроллера Elsys-MB-AC и имеющем похожие названия значений настроек.

#### 5.15.7 Настройка взаимодействий

Настройка взаимодействий и формул управления выходами выполняется точно так же, как для старших моделей контроллеров (см. п. 9.1), с учётом ряда ограничений, описанных ниже.

Логические формулы и служебные PIN-коды в Elsys-MB-AC не поддерживаются. В базу данных для каждого контроллера Elsys-MB-AC может быть добавлено до 50 взаимодействий и до 16 формул управления выходами.



В качестве источников событий могут быть использованы следующие устройства:

- контроллер (событие «сброс»; событие «сообщение от контроллера» - для настройки взаимодействий);
- входы;
- разделы.

В качестве объектов управления могут быть использованы следующие устройства:

- контроллер (команда «Сформировать сообщение контроллерам» – для настройки межконтроллерных взаимодействий);
- выход
- раздел;
- вход (при условии, что он не входит ни в один раздел).

### 5.16 Управление устройствами из конфигуратора оборудования

Управление устройствами, подключенными к драйверу, может осуществляться как с помощью контекстных меню пиктограмм устройств (см. Инструкцию оператора), так и из конфигуратора оборудования (вкладки **«Управление»** на страницах свойств устройств в дереве конфигурации, рисунки 83 -89), с любого сетевого места в сети комплекса. Первый способ используется при штатной эксплуатации системы, а второй следует использовать при первоначальной настройке системы, либо при ремонтно-диагностических работах. Описание команд управления и диапазон значений параметров управления представлен в п. 9.4.8 (см. таблица 32).

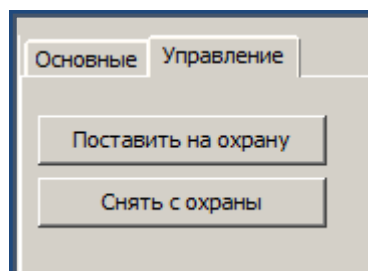


Рисунок 83- Управление входом

Основные Управление

Включить по формуле

Включить

Задержка 0

+ полупериод 1

- полупериод 0

Число повторений 1

Единица измерения 1 с

Выключить

Перебросить

Рисунок 84 - Управление выходом

Основные Состав группы Управление

Включить по формуле

Включить

Задержка 0

+ полупериод 1

- полупериод 0

Число повторений 1

Единица измерения 1 с

Выключить

Перебросить

Рисунок 85 - Управление группой выходов

Основные Управление

Открыть

Восстановить норм. режим

Заблокировать

Разблокировать

Рисунок 86 - Управление дверью

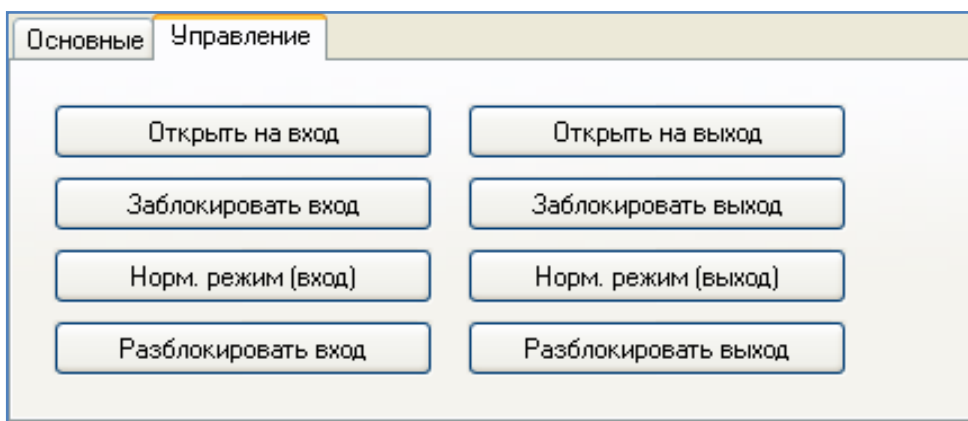


Рисунок 87 - Управление турникетом

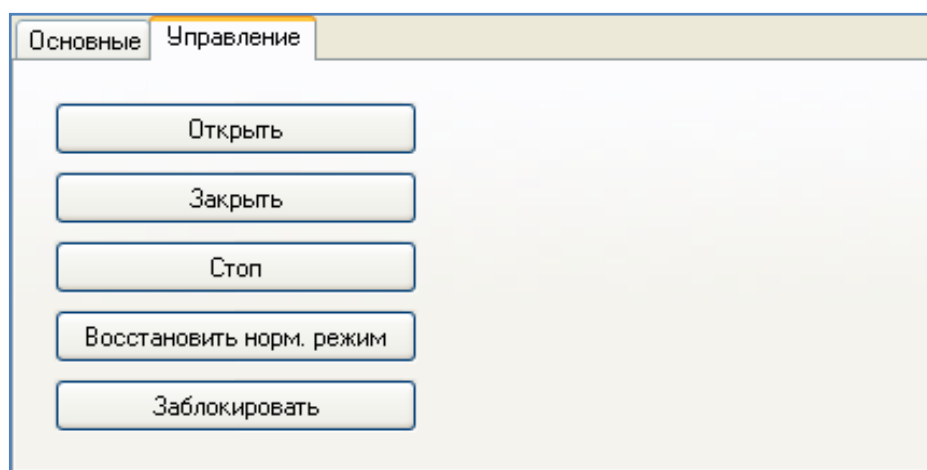


Рисунок 88 - Управление воротами или шлагбаумом

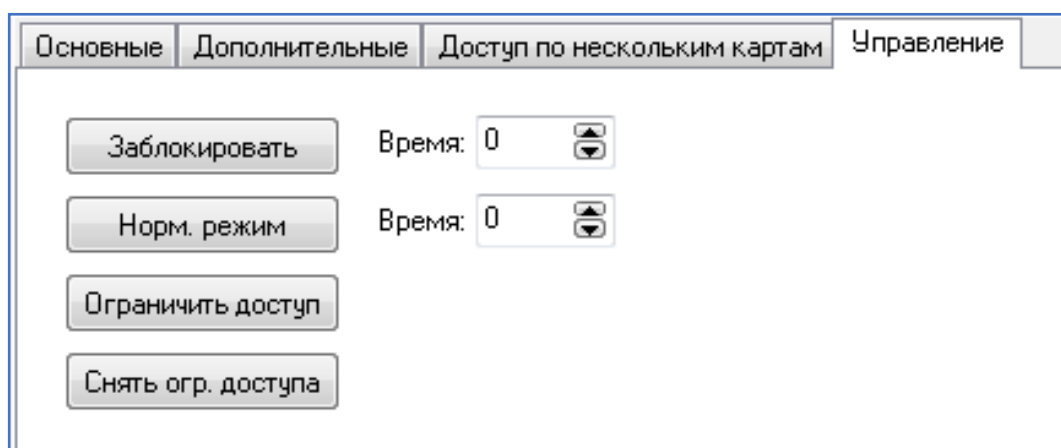


Рисунок 89 - Управление считывателем

### 5.17 Установка ограничений доступа к различным функциям драйвера

Установка ограничений доступа производится в окне «**Доступ к устройствам**», в котором для каждого профиля оператора можно установить доступность к функциям драйвера, а также доступность команд управления устройствами драйвера (рисунок 90).

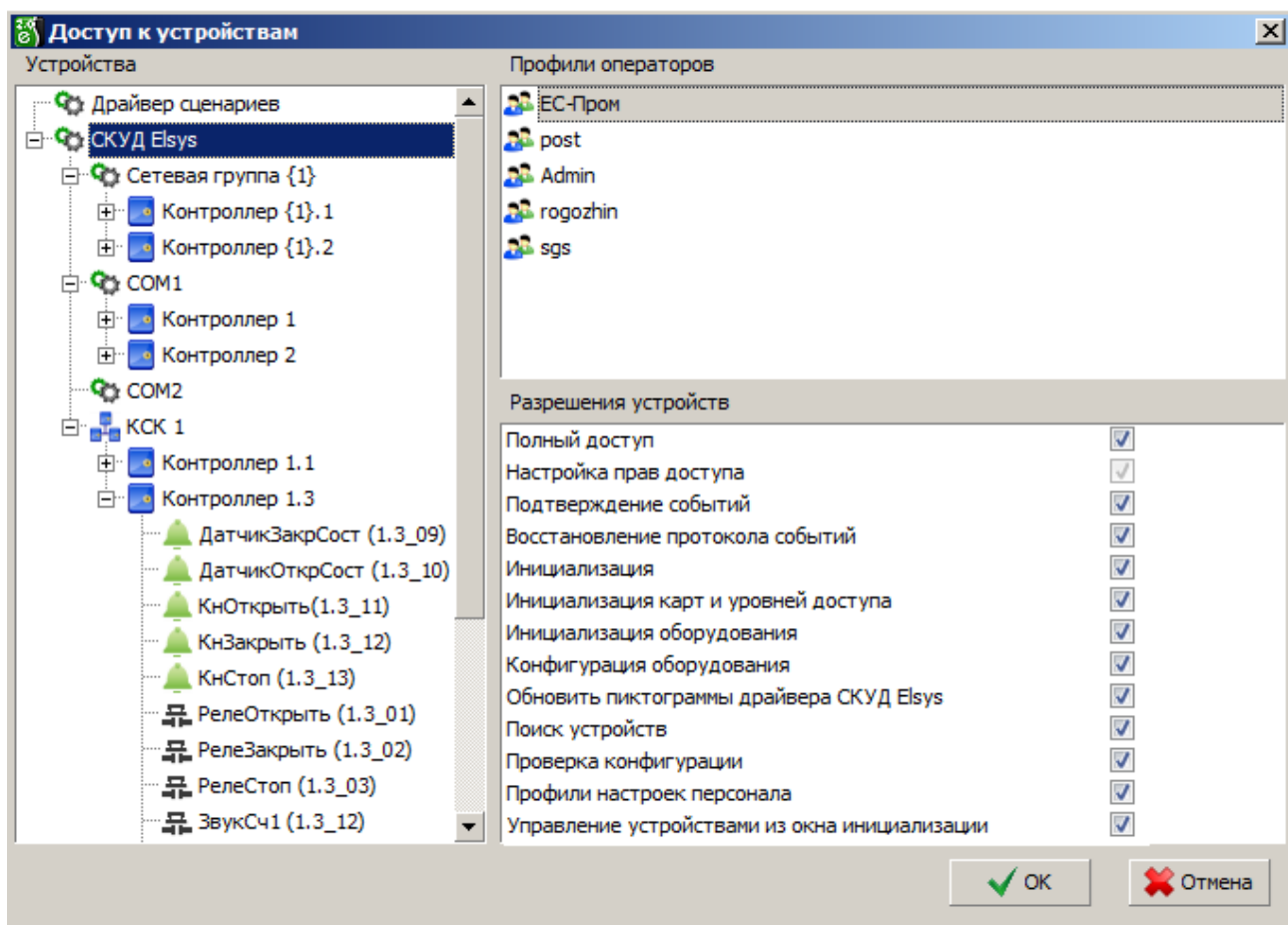


Рисунок 90 - Установка доступа к функциям драйвера «Бастион-2 – Elsys»

Чтобы вызывать окно «Доступ к устройствам» следует в главном окне «Бастион-2» перейти на вкладку «Конфигурация» и на ленте «Операторы и полномочия» нажать кнопку «Доступ к устройствам» (рисунок 91).

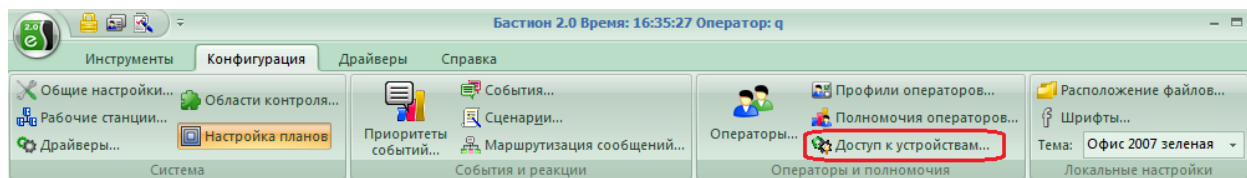


Рисунок 91 - Вызов окна «Доступ к устройствам»

Далее, следует в появившемся окне в дереве устройств выбрать узел типа драйвера «СКУД Elsys», профиль оператора и установить требуемые разрешения. Разрешения, устанавливаемые для типа драйвера, являются общими для всех экземпляров драйверов этого типа, установленных в системе.

«**Полный доступ**» - разрешает пользователю выполнять все функции ПО «Бастион-2»

«**Настройка прав доступа**» - разрешает пользователю выполнять настройку разрешений в окне «Доступ к устройствам».

«**Подтверждение событий**» - разрешает пользователю выполнять подтверждение тревожных событий.

**«Восстановление протокола событий»** - устанавливает доступность одноимённой кнопки на панели управления драйвером.

**«Инициализация»** - устанавливает доступность одноимённой кнопки на панели управления драйвером.

**«Инициализация карт и уровней доступа»** - разрешает пользователю производить инициализацию праздников, временных блоков, уровней доступа и карт доступа в режиме инициализации.

**«Инициализация оборудования»** - разрешает оператору производить инициализацию даты и времени и оборудования в режиме инициализации.

**«Конфигурация оборудования»** - устанавливает доступность одноимённой кнопки на панели управления драйвером.

**«Обновить пиктограммы драйвера СКУД Elsys»** - устанавливает доступность одноимённой кнопки на панели управления драйвером.

**«Поиск устройств»** - устанавливает доступность одноимённой кнопки на панели управления драйвером.

**«Проверка конфигурации»** - устанавливает доступность одноимённой кнопки на панели управления драйвером.

**«Профили настроек персонала»** - устанавливает доступность одноимённой кнопки на панели управления драйвером.

**«Управление устройствами из окна инициализации»** - разрешает управление контроллером в режиме инициализации (подробнее см. п. 5.16).

## **6 Настройка глобального контроля последовательности прохода**

### **6.1 Описание работы глобального контроля последовательности прохода**

Контроль последовательности прохода (antipassback) обеспечивает защиту от повторного использования идентификатора в одном направлении и позволяет выявлять и предупреждать такие нарушения дисциплины, как передача карты другому лицу и проход сотрудников вне точек доступа.

В контроллерах Elsys-MB может использоваться либо локальный, либо глобальный antipassback.

Локальный antipassback может использоваться, если две области контроля разделены одной или двумя (при использовании Pro4) точками доступа, и их обслуживает единственный контроллер. Для включения локального контроля последовательности прохода следует установить настройку контроллера **«Использование контроля последовательности прохода»** в значение **«Использовать локальный контроль**

**последовательности прохода»** (рисунок 43). Одновременно использовать локальный и глобальный antipassback нельзя.

Если контроль последовательности прохода должны обеспечивать нескольких контроллеров, следует использовать глобальный antipassback.

При использовании функции **«Глобальный контроль последовательности прохода»** следует учитывать следующие ограничения:

- каждый контроллер доступа может обслуживать не более двух областей контроля (четыре для Pro4 с версией прошивки 2.66 и выше);
- контроллеры Elsys-MB-SM поддерживают функцию antipassback (как глобальный, так и локальный), если в памяти контроллера содержится не более 150 карт доступа.

Глобальный antipassback функционирует в пределах единого информационного пространства, в котором возможен обмен информацией между контроллерами. Единое информационное пространство может быть создано:

- в любой линии связи RS-485, подключенной к COM-порту или КСК Elsys-MB-Net (до 63 УУ Elsys-MB);
- в любой сетевой группе, включающей до 63 УУ Elsys-MB-IP;
- при использовании КСК Elsys-MB-Net – в совокупности всех УУ, обслуживаемых ими.

Каждый КСК Elsys-MB-Net может обслуживать одну линию связи RS-485 (до 63 УУ Elsys-MB) и/или одну сетевую группу (до 63 УУ Elsys-MB-IP). Суммарное число линий связи и сетевых групп в одной системе может достигать 240.

Глобальный контроль последовательности прохода работает децентрализованно, без участия компьютера или какого-либо ведущего устройства, что обеспечивает высокую надёжность работы этой функции.

Для работы глобального контроля последовательности прохода всю территорию предприятия, обслуживаемую СКУД, необходимо условно разделить на области контроля (термины «область контроля» и «зона доступа», используемые в СКУД Elsys и ПО «Бастион-2», равнозначны). По умолчанию в конфигураторе областей контроля существуют две области контроля **«На территории»** и **«Вне территории»**. Для более сложных конфигураций могут быть созданы дополнительные области контроля. Вложенность областей контроля роли не играет, так как для работы функции antipassback достаточно иметь информацию о том, через какие точки доступа области контроля граничат друг с другом.

Вход и выход в каждую область контроля должен осуществляться исключительно через точки доступа (двери, ворота, турникеты). Для каждой из этих точек доступа должны быть назначены внешняя (т. е. откуда осуществляется вход и куда осуществляется выход) и внутренняя (куда осуществляется вход и откуда осуществляется выход) области контроля. Для некоторых точек доступа (в том числе односторонних) возможно задание одной и той

же области контроля в качестве входной и выходной – в этом случае считается, что точка доступа находится внутри области контроля.

Каждый контроллер в режиме глобального контроля последовательности прохода может обслуживать не более двух областей контроля (четырёх для Pro4 с прошивкой 2.66 и выше). Для точек доступа, обслуживаемых контроллером, любая из этих областей контроля может быть назначена как внешняя или как внутренняя.

Контроллеры, входящие в единое информационное пространство, обмениваются с другими контроллерами сообщениями о фактически совершённых проходах. В начальный момент времени каждый сотрудник имеет право проходить в любом направлении. После каждого совершённого прохода всем контроллерам известно местоположение сотрудника – его текущая область контроля. Сотрудник имеет право на перемещение из области контроля, где он был последний раз зарегистрирован, в другую область контроля, а также право на перемещения внутри области контроля (т. е. в точках доступа, где входная и выходная область контроля совпадают). Если сотрудник предъявит карту в любой другой области контроля (например, совершив проход без предъявления карты, или передав карту другому лицу), в доступе ему будет отказано, с одновременной регистрацией сообщения «Нарушение зоны доступа».

В соответствии с текущей областью контроля, все контроллеры регистрируют в своей памяти местоположение каждого сотрудника, изменяя внутренний параметр «*Зона доступа*».

Этот параметр, определяющий разрешённые направления прохода (условно обозначаемые «Вход» и «Выход»), может принимать одно из четырёх значений:

- «*Разрешён вход и выход*». Это значение параметр принимает в тех случаях, когда точное местоположение сотрудника для контроллера неизвестно (после сброса, инициализации базы данных пользователей или областей контроля, нарушений связи и т.п.);
- "*Разрешён выход, вход запрещён*". Это значение параметр принимает, если пользователь находится во внутренней области контроля;
- "*Разрешён вход, выход запрещён*". Это значение параметр принимает, если пользователь находится во внешней области контроля;
- "*Запрещён вход и выход*". Это значение параметр принимает, если пользователь находится в зоне, не обслуживаемой этим контроллером.

При использовании глобального контроля последовательности прохода следует учитывать, что в перечисленных ниже случаях выполняется сброс областей контроля в контроллерах (для карт доступа устанавливается состояние "*Разрешён вход и выход*"):

- после выполнения из окна инициализации команды «Сброс антипасбэка», адресованной конкретному контроллеру;

- после сброса или выключения питания контроллера;
- после потерь связи с другими контроллерами (если выключена опция «Не отслеживать исправность областей контроля»);
- после инициализации оборудования, карт доступа, областей контроля;
- после редактирования областей контроля (т. к. вслед за этим следует автоматическая инициализация областей контроля);
- после изменения настроек АПБ для КСК, сетевой группы, СОМ-порта или отдельного контроллера (в этом случае после сохранения настроек происходит перезапуск драйвера и автоматическая инициализация АПБ во всех устройствах);
- после редактирования свойств пропуска – только для конкретного пропуска;
- в полночь (если включена настройка «Сброс в полночь»);
- по функции «временной antipassback» – для конкретных пропусков отдельно.

Для работы глобального контроля последовательности прохода необходимо:

- назначить адреса контроллерам по порядку, без пропусков (в каждой линии связи RS-485 адреса должны начинаться с «1», т.к. наличие пропусков адресах, нумерация не с «1», исключенные из опроса контроллеры, приводят к снижению скорости работы системы в режиме Multimaster);
- обновить прошивки контроллеров (использование контроллеров Elsys-MB с версией прошивки ниже 2.63 и Elsys-SM версии ниже 2.20 приведёт к снижению быстродействия системы);
- настроить единое информационное пространство, включив antipassback и обмен данными между контроллерами (п. 6.2);
- настроить области контроля (п. 6.3);
- проверить корректность настройки оборудования для работы глобального контроля последовательности прохода с учетом настроек областей контроля (п. 6.4);
- выполнить, если необходимо, дополнительные настройки (п. 6.5).

## **6.2 Настройка оборудования для работы глобального контроля последовательности прохода**

Чтобы обеспечить обмен данными между контроллерами, входящими в единое информационное пространство, должны быть выполнены следующие настройки:

- 1) установлены взаимосвязи КСК Elsys-MB-Net и сетевых групп (если они используются и участвуют в едином информационном пространстве);



- 2) режим обмена в линии связи RS-485 - MULTIMASTER;
- 3) обмен информацией всех контроллеров в сетевой группе между собой - включен;
- 4) обмен информацией КСК Elsys-MB-Net между собой - включен;
- 5) глобальный контроль последовательности прохода в каждой линии связи и сетевой группе – включен.

Настройки, упомянутые в п. 2) – 4) включаются автоматически при включении настройки «Глобальный контроль последовательности прохода» в соответствующих линиях связи (СОМ-порт, КСК Elsys-MB-Net, сетевая группа). Если единое информационное пространство охватывает все КСК Elsys-MB-Net, наиболее простой способ включить обмен данными – нажать кнопку **«Включить во всех КСК»**, после чего будут включены настройки, упомянутые в п. 2) – 5) (см. п. 6.2.2).

Все контроллеры, участвующие в работе глобального контроля последовательности прохода, должны иметь настройку **«Использование контроля последовательности прохода»** в значении «Использовать в соответствии с настройками драйвера/ сетевого контроллера/ сетевой группы» (по умолчанию), обеспечивающем групповое управление режимом **«Глобальный контроль последовательности прохода»**.

Если контроллер необходимо исключить из глобального контроля последовательности прохода следует установить настройку контроллера **«Использование контроля последовательности прохода»** в значение **«Не использовать»**.

При настройке обмена данными КСК Elsys-MB-Net между собой, а также контроллеров Elsys-MB-IP в сетевой группе используется групповая опция **«Режим передачи данных»**, которая может принимать значения **«По подсетям»**, **«Адресный»**, **«Широковещательный»**. В первом случае при обмене информацией между контроллерами используются пакеты с адресом подсети (например, 192.168.1.255), во втором случае используются адресные пакеты, в третьем - широковещательные пакеты (с IP-адресом получателя 255.255.255.255). По умолчанию используется режим **«По подсетям»**. Если в сети запрещены широковещательные пакеты, следует включить режим **«Адресный»**.

Кроме выполнения настроек в ПО «Бастион-2», для обеспечения обмена данными КСК Elsys-MB-Net между собой, а также контроллеров Elsys-MB-IP в сетевых группах, необходимо обеспечить, чтобы в локальной сети предприятия были разрешены используемые этими устройствами TCP и UDP порты (см. документацию на КСК Elsys-MB-Net и модуль Elsys-IP).

### 6.2.1 Настройка в одной линии связи

Включение и выключение глобального контроля последовательности прохода можно выполнить в свойствах узла каждой линии связи дерева конфигурации в группе элементов управления **«Глобальный контроль последовательности прохода»** (рисунки 23, 29, 30).

Чтобы включить функцию **«Глобальный контроль последовательности прохода»** следует нажать кнопку **«Включить antipassback»**, чтобы выключить данную функцию следует нажать кнопку **«Выключить antipassback»**.

При включении функции antipassback в линии связи сетевого контроллера и COM-порта автоматически включается режим обмена **«MULTIMASTER»**, что необходимо для работы функции antipassback.

При выключении функции antipassback автоматического переключения режима обмена не происходит и, если обмен между контроллерами в линии связи не требуется, то следует установить режим **«MASTER-SLAVE»**.

К работе функции antipassback также относятся опции **«Не проверять исправность областей контроля»** и **«Усиленный antipassback»**, которые подробно описаны в п. 6.5.

### 6.2.2 Настройка в линиях связи сетевых контроллеров

Для линий связи сетевых контроллеров существует возможность настройки функции antipassback сразу для всех КСК, относящихся к одному серверу оборудования, или выборочно для каждой линии КСК.

Все параметры настройки функции antipassback в нескольких линиях КСК, относящихся к одному серверу оборудования, находятся в свойствах узла **«Коммуникационные контроллеры»**, соответствующего сервера оборудования (рисунок 92).

Основные | Области контроля

Режим передачи данных

- По подсетям (по умолчанию)
- Широковещательный
- Адресный

Глобальный контроль последовательности прохода

Включить во всех КСК    Выключить во всех КСК

Глобальный antipassback включен.

Настройка обмена данными между коммуникационными контроллерами на сервере оборудования "AGAFONOVA"

№	Коммуникационный контроллер	MultMaster в линии RS-485	Antipassback в линии RS-485	Обмен с другими КСК	Глобальный antipassback	Диагностика настройки	Не проверять обл. контроля	Усиленный antipassback
1	КСК 1 (ЦП) - Сетевая группа {1}	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Глобальный antipassback включен.	<input type="checkbox"/>	<input type="checkbox"/>
2	КСК 2 (ЮП)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Глобальный antipassback включен.	<input type="checkbox"/>	<input type="checkbox"/>
Все КСК		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Глобальный antipassback включен.	<input type="checkbox"/>	<input type="checkbox"/>

Рисунок 92 – Окно свойств узла «Коммуникационные контроллеры»

**«Глобальный контроль последовательности прохода»** - группа элементов управления, которая позволяет включать и выключать режим глобального контроля последовательности прохода сразу во всех КСК, относящихся к текущему серверу оборудования, а также выводит текстовую информацию о корректности его настройки.

**«Настройка обмена данными между коммуникационными контроллерами на сервере оборудования»** - таблица для отображения и редактирования настроек обмена между КСК, относящихся к текущему серверу оборудования. Опции в таблице можно устанавливать как для одного КСК, в соответствующей строке, так и для всех КСК, в строке **«Все КСК»**.

Если КСК включен в сетевую группу, то наименование сетевой группы выводится вместе с наименованием КСК в столбце **«Коммуникационный контроллер»**.

Опция в столбце **«MultiMaster в линии RS-485»** служит для включения (выключения) режима обмена в линии связи RS-485.

Опция в столбце **«Antipassback в линии RS-485»** служит для включения (выключения) функции antipassback в линии связи RS-485 сетевого контроллера.

Опция в столбце **«Обмен с другими КСК»** служит для включения (отключения) обмена информацией КСК Elsys-MB-Net между собой.

Опция в столбце **«Глобальный antipassback»** служит для включения (выключения) глобального контроля последовательности прохода в сетевом контроллере.

При включении опции **«Глобальный antipassback»** автоматически включаются все опции, необходимые для работы глобального контроля последовательности прохода:

- **«MultiMaster в линии RS-485»;**
- **«Antipassback в линии RS-485»;**
- **«Обмен с другими КСК».**

При выключении опции **«Глобальный antipassback»** автоматического выключения опций **«MultiMaster в линии RS-485»** и **«Обмен с другими КСК»** не происходит, и если требуется их также можно отключить.

Опции в столбцах **«Не проверять обл. контроля»** и **«Усиленный antipassback»** служат для включения (выключения) дополнительных настроек функции antipassback: **«Не проверять исправность областей контроля»** и **«Усиленный antipassback»**, соответственно (см. п. 6.5).

***Внимание!** После редактирования настроек, относящихся к настройке глобального контроля последовательности прохода, при выходе из конфигуратора автоматически запускается инициализация областей контроля.*

### 6.3 Настройка областей контроля

Для работы глобального контроля последовательности прохода необходимо сконфигурировать области контроля (рисунок 93).

В появившемся окне (рисунок 94) необходимо указать из какой и в какую область контроля ведет каждая точка доступа. На рисунке приведён пример настройки областей контроля для предприятия, схема которого приведена на рисунке 103.

Подробное описание настройки областей контроля дано в «Руководстве администратора «Бастион-2».

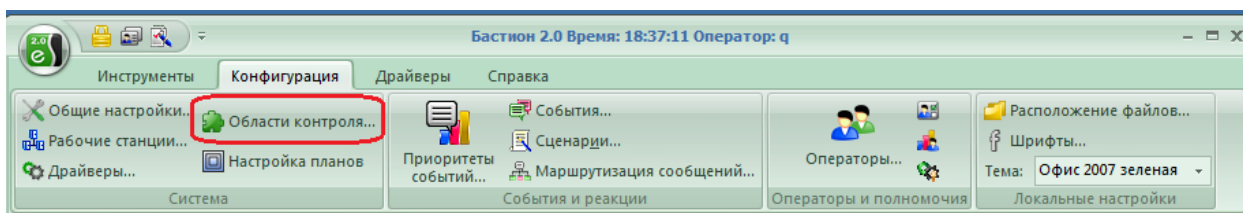


Рисунок 93 – Вызов окна настройки областей контроля

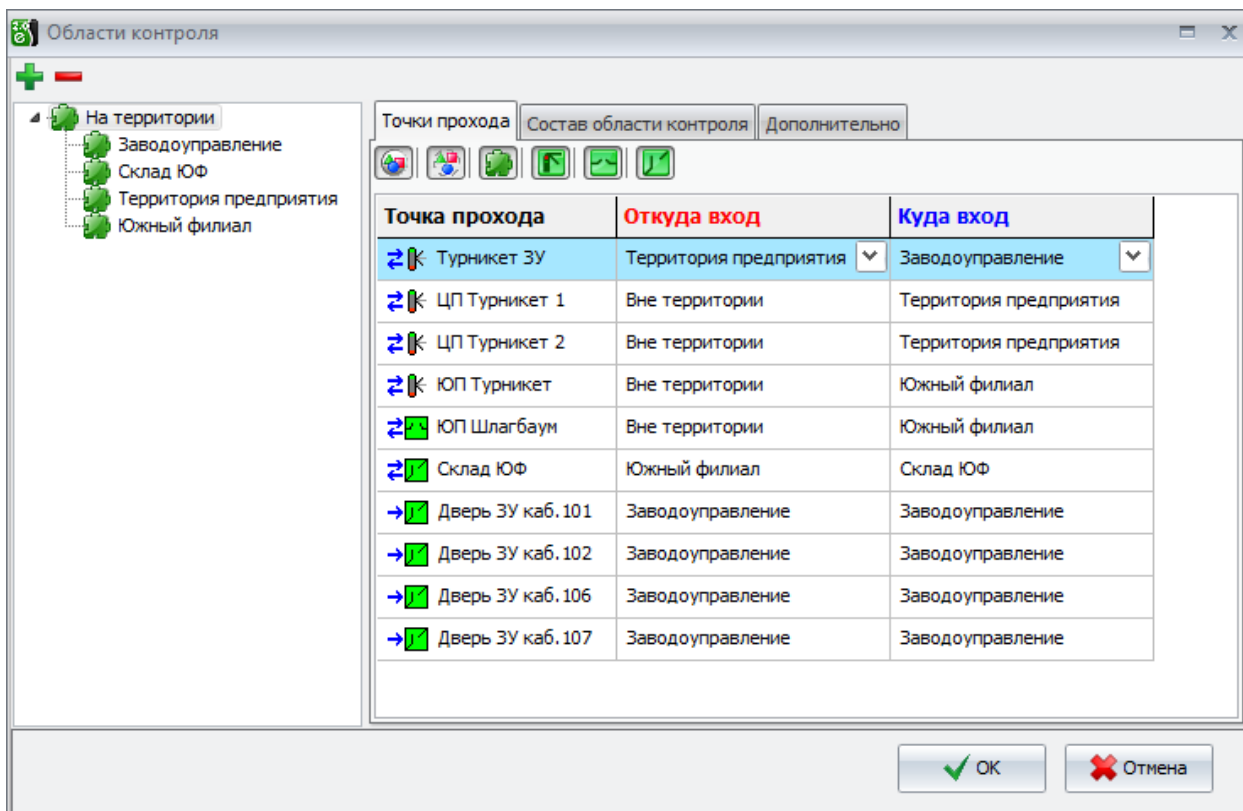


Рисунок 94 – Окно настройки областей контроля

## 6.4 Диагностика глобального контроля последовательности прохода

При включенной настройке «Глобальный контроль последовательности прохода» в конфигураторе драйвера «Бастион-2 – Elsys» проверяется корректность настройки оборудования для работы глобального контроля последовательности прохода с учетом настроек областей контроля.

Результаты проверки отображаются в разрезе областей контроля, а также для каждой линии связи.

Чтобы проверить корректность настройки глобального контроля последовательности прохода следует открыть окно свойств узла «Коммуникационные контроллеры» дерева конфигурации и перейти на страницу свойств «Области контроля». В таблице

«**Диагностика настройки глобального контроля последовательности прохода**» выводится список всех областей контроля, в которых задействованы точки прохода СКУД Elsys.

Если ошибок в настройке не обнаружено, то в таблице для всех областей контроля в столбце «**Диагностика области контроля**» выводится текстовое сообщение «Ошибок не обнаружено» (рисунок 95).

Основные		Области контроля
<b>Диагностика настройки глобального контроля последовательности прохода</b>		
№	Наименование области контроля	Диагностика области контроля
1	Вне территории	Ошибок не обнаружено
2	Южный филиал	Ошибок не обнаружено
3	Заводоуправление	Ошибок не обнаружено
4	Склад ЮФ	Ошибок не обнаружено
5	Территория предприятия	Ошибок не обнаружено
<b>Все области контроля</b>		<b>Ошибок не обнаружено</b>

Рисунок 95– Корректная настройка глобального контроля последовательности прохода

При обнаружении ошибок в таблице кроме диагностики области контроля выводится также линия связи (столбец «**Источник ошибки**»), в которой обнаружена ошибка и причина ошибки (рисунок 96). Источник ошибки в таблице отображается в виде гиперссылки, с помощью которой можно перейти в окно свойств линии связи, в которой произошла ошибка (рисунки 97 - 98) и скорректировать настройки. Чтобы обновить диагностику с учетом изменений необходимо сохранить изменения в базе данных, нажав кнопку «Применить» на панели инструментов драйвера.

Основные		Области контроля		
<b>Диагностика настройки глобального контроля последовательности прохода</b>				
№	Наименование области контроля	Диагностика области контроля	Источник ошибки	Причина ошибки
1	Вне территории	Выключен antipassback в некоторых линиях связи	<a href="#">КСК 2 (ЮП)</a>	Выключен обмен с другими коммуникационными контроллерами
2	Южный филиал	Ошибка не обнаружено		
3	Заводоуправление	Выключен antipassback		
4	Склад ЮФ	Ошибка не обнаружено		
5	Территория предприятия	Выключен antipassback в некоторых линиях связи	<a href="#">Сетевая группа {1}</a>	Выключен antipassback
<b>Все области контроля</b>		<b>Обнаружены ошибки</b>		

Рисунок 96– Обнаруженные ошибки настройки глобального контроля последовательности прохода

Основные		Дополнительные		Области контроля																
Наименование КСК:	<input type="text" value="КСК 2 (ЮП)"/>	Номер:	<input type="text" value="2"/>	Входит в сетевую группу:	<input type="text" value="(Нет)"/>															
		Версия:	<input type="text" value="2.08"/>																	
<b>Настройки для линии связи RS-485 сетевого контроллера</b>			<b>Использование контроля последовательности прохода в контроллерах доступа</b>																	
Глобальный контроль последовательности прохода <input type="button" value="Включить antipassback"/> <input type="button" value="Выключить antipassback"/> Глобальный antipassback включен частично. Выключен обмен данными с другими КСК. Обнаружены ошибки в областях контроля. <input type="checkbox"/> Усиленный antipassback			<table border="1"> <thead> <tr> <th>№</th> <th>Наименование контроллера</th> <th>Контроль последовательности прохода</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Контроллер 2.1 ЮИ</td> <td>Глобальный antipassback</td> </tr> <tr> <td>2</td> <td>Контроллер 2.2 ЮИ</td> <td>Глобальный antipassback</td> </tr> <tr> <td>3</td> <td>Склад ЮФ (2.3)</td> <td>Глобальный antipassback</td> </tr> <tr> <td colspan="2"><b>Все контроллеры</b></td> <td>Используется глобальный antipassback</td> </tr> </tbody> </table>			№	Наименование контроллера	Контроль последовательности прохода	1	Контроллер 2.1 ЮИ	Глобальный antipassback	2	Контроллер 2.2 ЮИ	Глобальный antipassback	3	Склад ЮФ (2.3)	Глобальный antipassback	<b>Все контроллеры</b>		Используется глобальный antipassback
№	Наименование контроллера	Контроль последовательности прохода																		
1	Контроллер 2.1 ЮИ	Глобальный antipassback																		
2	Контроллер 2.2 ЮИ	Глобальный antipassback																		
3	Склад ЮФ (2.3)	Глобальный antipassback																		
<b>Все контроллеры</b>		Используется глобальный antipassback																		
Скорость обмена, бит/с:	<input type="text" value="38400"/>	Режим обмена	<input type="radio"/> MASTER - SLAVE <input checked="" type="radio"/> MULTIMASTER																	

Рисунок 97– Диагностика ошибок в линии связи КСК

Основные **Области контроля**

Наименование сетевой группы:  Номер:  UDP-порт:

Группа содержит КСК:   Не проверять исправность областей контроля

**Режим передачи данных**

По подсетям (по умолчанию)  
 Широковещательный  
 Адресный

**Глобальный контроль последовательности прохода**

Глобальный antipassback выключен.  
Обнаружены ошибки в областях контроля.

Усиленный antipassback

**Настройка обмена данными между контроллерами в сетевой группе**

№	Контроллер	Использование контроля последовательности прохода	Обмен с контроллерами	Antipassback в управляющем КСК: "КСК 1 (ЦП)"
1	ЗУ Вход {1}.1	Глобальный antipassback.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> Обмен данными с другими КСК <input checked="" type="checkbox"/> Antipassback в линии RS-485 <input checked="" type="checkbox"/> Глобальный antipassback <b>Глобальный antipassback включен.</b>
2	ЗУ каб. 101, 102 {1}.2	Глобальный antipassback.	<input checked="" type="checkbox"/>	
3	ЗУ каб. 106, 107 {1}.3	Глобальный antipassback.	<input checked="" type="checkbox"/>	
<b>Все контроллеры</b>		Глобальный antipassback	<input checked="" type="checkbox"/>	

Рисунок 98– Диагностика ошибок в сетевой группе

В окне свойств узла «Коммуникационные контроллеры» на странице «Основные» результаты диагностики выводятся для всех линий связи сетевых контроллеров, относящихся к текущему серверу (рисунок 99).

Основные **Области контроля**

**Режим передачи данных**

По подсетям (по умолчанию)  
 Широковещательный  
 Адресный

**Глобальный контроль последовательности прохода**

Глобальный antipassback включен частично.  
Выключен обмен данными с некоторыми КСК.  
Обнаружены ошибки в областях контроля.

**Настройка обмена данными между коммуникационными контроллерами на сервере оборудования "AGAFONOVA"**

№	Коммуникационный контроллер	MultiMaster в линии RS-485	Antipassback в линии RS-485	Обмен с другими КСК	Глобальный antipassback	Диагностика настройки	Не проверять обл. контроля	Усиленный antipassback
1	КСК 1 (ЦП) - Сетевая	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Глобальный antipassback включен частично. Выключен antipassback в СГ. Обнаружены ошибки в областях контроля.	<input type="checkbox"/>	<input type="checkbox"/>
2	КСК 2 (ЮП)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Глобальный antipassback включен частично. Выключен обмен данными с другими КСК. Обнаружены ошибки в областях контроля.	<input type="checkbox"/>	<input type="checkbox"/>
<b>Все КСК</b>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Глобальный antipassback включен частично. Выключен обмен данными с некоторыми КСК. Обнаружены ошибки в областях контроля.	<input type="checkbox"/>	<input type="checkbox"/>

Рисунок 99– Диагностика ошибок во всех КСК, относящихся к текущему серверу оборудования



В свойствах каждой линии связи на вкладке «Области контроля» выводятся результаты диагностики областей контроля, обслуживаемых данной линией связи, а также диагностика этих областей контроля в разрезе текущей линии связи (рисунки 100 -101).

№	Наименование области контроля	Диагностика в текущем КСК	Диагностика области контроля
1	Вне территории	Выключен обмен с другими коммуникационными контроллерами	Выключен antipassback в некоторых линиях связи
2	Южный филиал	Выключен обмен с другими коммуникационными контроллерами	Ошибок не обнаружено
3	Склад ЮФ	Выключен обмен с другими коммуникационными контроллерами	Ошибок не обнаружено
<b>Все области контроля</b>		<b>Обнаружены ошибки</b>	<b>Обнаружены ошибки</b>

**Рисунок 100– Диагностика настройки глобального контроля последовательности прохода в линии связи КСК в разрезе областей контроля**

№	Наименование области контроля	Диагностика в текущей СГ	Диагностика области контроля
1	Заводоуправление	Выключен antipassback	Выключен antipassback
2	Территория предприятия	Выключен antipassback	Выключен antipassback в некоторых линиях связи
<b>Все области контроля</b>		<b>Обнаружены ошибки</b>	<b>Обнаружены ошибки</b>

**Рисунок 101– Диагностика настройки глобального контроля последовательности прохода в сетевой группе в разрезе областей контроля**

**Внимание!** После изменения настроек оборудования, связанных с работой глобального контроля последовательности прохода, обновление результатов диагностики происходит после сохранения изменений в базе данных.

## 6.5 Дополнительные настройки глобального контроля последовательности прохода

Для работы глобального контроля последовательности прохода могут потребоваться дополнительные настройки. Их описание дано в настоящей главе.

### 6.5.1 Мягкий antipassback

Если при использовании контроля последовательности прохода необходимо, регистрируя нарушение, автоматически предоставлять доступ, следует в свойствах считывателей включить настройку «Предоставлять доступ при нарушении зоны доступа» (рисунок 76). Настройка вступает в силу после инициализации контроллеров доступа (должна быть выбрана группа настроек «Оборудование»).



### 6.5.2 Настройка «Сброс в полночь»

Чтобы предотвратить возможные необоснованные отказы в доступе, рекомендуется по истечении определённого времени выполнять автоматический сброс текущей области контроля для всех (или отдельных) сотрудников.

Это можно сделать, включив в контроллерах доступа, где это необходимо, настройку **«Сброс в полночь»** (рисунок 43). Если эта настройка включена, то в 0 час 0 мин в контроллерах ежедневно будет очищаться информация о текущей зоне доступа всех сотрудников.

### 6.5.3 Временной antipassback

Суть временного контроля последовательности прохода – сброс текущей зоны доступа для каждого конкретного сотрудника спустя заданное время после совершения им последнего прохода.

Режим временного контроля последовательности прохода может быть включен для контроллеров старших моделей (Light, Standard, Pro, Pro4), имеющих номер версии встроенного ПО 2.53 или старше и установленный модуль расширения памяти. Кроме того, для работы этого режима должна быть включена опция контроллера **«Расширенные возможности настройки»** (рисунок 36) и задана настройка **«Интервал через который сбрасывается информация о прошедшей карте, мин»** (рисунок 42).

Описанные настройки вступают в силу после инициализации контроллеров доступа (должна быть выбрана группа настроек **«Оборудование»**).

Временной antipassback может использоваться для автоматического сброса текущего местоположения сотрудников, если нежелательно использовать настройку **«Сброс в полночь»** (например, для предприятий с круглосуточным режимом работы), а также в некоторых других случаях.

### 6.5.4 Настройка «Не проверять исправность областей контроля»

Настройка **«Не проверять исправность областей контроля»** (рисунок 23) определяет алгоритм работы функции antipassback при потерях связи с контроллерами.

По умолчанию, если настройка выключена, все контроллеры непрерывно анализируют исправность обслуживаемых ими областей контроля. Если хотя бы с одним из контроллеров, обслуживающих область контроля, отсутствует связь, область контроля считается неисправной. Если хотя бы одна область контроля неисправна, antipassback в контроллере прекращает работать, при этом для всех сотрудников выполняется сброс текущего местоположения.

Этот механизм предотвращает возможные необоснованные отказы в доступе, если из-за нарушений связи не все контроллеры получают информацию о текущем местоположении сотрудников.

Если настройка **«Не проверять исправность областей контроля»** включена, сброс текущего местоположения пользователей при нарушениях связи не выполняется. Тем самым обеспечивается сохранение работоспособности функции antipassback при

кратковременных и длительных нарушениях связи, однако становятся возможными необоснованные отказы в доступе.

В конфигураторе СКУД Esys настройка **«Не проверять исправность областей контроля»** присутствует в окнах свойств COM-порта, коммуникационного сетевого контроллера и сетевой группы, а также в окне групповой настройки свойств коммуникационных контроллеров. Настройка вступает в силу после инициализации всех контроллеров Esys-MB, относящихся к соответствующим линиям связи или сетевым группам, и после инициализации всех КСК Esys-MB-Net, где она была изменена. Если используются контроллеры Esys-MB версий 2.60 и выше, а также контроллеры Esys-MB-Net версий 2.08 и выше, настройка загружается в контроллеры автоматически, после выхода из конфигуратора.

### 6.5.5 Настройка **«Усиленный antipassback»**

**«Усиленный antipassback»** – режим, обеспечивающий дополнительную защиту от несанкционированного доступа. Суть его заключается в следующем. В обычном режиме (если настройка **«Усиленный antipassback»** выключена) сообщения об изменении зоны доступа рассылаются другим контроллерам после регистрации фактического прохода (в момент срабатывания датчика прохода). Нарушитель может, успев за время, отводимое на проход, предъявить на проходной карту нескольким считывателям, провести на территорию предприятия посторонних лиц. Для предотвращения такой ситуации можно настроить систему, чтобы проход регистрировался одновременно с предъявлением карты. Но в этом случае, сотруднику, предъявившему карту, но по каким-то причинам не успевшему совершить проход, в следующий раз в доступе будет отказано. Режим **«Усиленный antipassback»**, будучи свободным от этого недостатка, предотвращает проход нескольких лиц по одной карте. В момент предъявления карты контроллер передаёт сообщение об изменении её текущей зоны доступа, а если проход не состоялся – сообщение о восстановлении текущей зоны доступа.

Режим **«Усиленный antipassback»** возможен для контроллеров Esys-MB старших моделей (Pro, Standard, Light, Pro4) версий 2.60 и выше. КСК Esys-MB-Net, обеспечивающие обмен данными, должны иметь версию не ниже 2.08.

В конфигураторе СКУД Esys настройка **«Усиленный antipassback»** присутствует в свойствах COM-порта (рисунок 30), коммуникационного сетевого контроллера (рисунок 23) и сетевой группы (рисунок 29), а также в окне групповой настройки свойств коммуникационных контроллеров (рисунок 92). Настройка загружается в контроллеры Esys-MB, относящиеся к соответствующим линиям связи или сетевым группам, и в КСК Esys-MB-Net, где она была изменена, автоматически, после выхода из конфигуратора.

### 6.5.6 Индивидуальная настройка **«не отслеживать последовательность прохода»**

Для отдельных пользователей системы (VIP-персоны, персонал, по служебной необходимости совершающий перемещения вне точек доступа, и т. п.) antipassback может быть отключен установкой индивидуальной опции пропуска **«Не отслеживать последовательность прохода»** на вкладке **«Пропуск»** (рисунок 102).

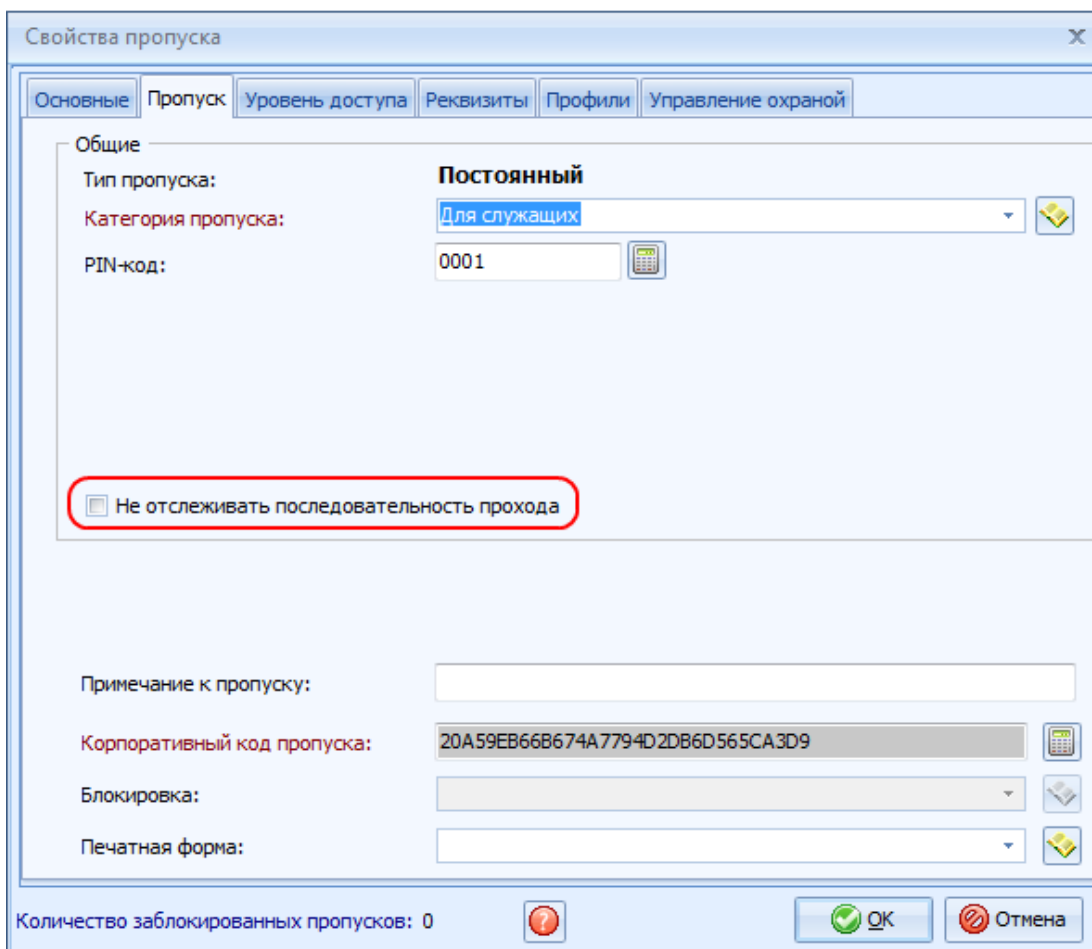


Рисунок 102 – Настройка «Не отслеживать последовательность прохода» в свойствах пропуска

## 6.6 Пример настройки глобального контроля последовательности прохода

Рассмотрим пример настройки глобального контроля последовательности прохода для предприятия, схема территории которого изображена на рисунке 103.

Территория предприятия состоит из главной производственной площадки, вход на которую осуществляется через центральную проходную (точки доступа «Турникет ЦП 1» и «Турникет ЦП 2»), и южного филиала, вход в который осуществляется через южную проходную (точки доступа «ЮП Турникет» и «ЮП шлагбаум»).

На территории главной производственной площадки расположено заводоуправление (ЗУ), вход в которое осуществляется через «Турникет ЗУ».

В заводоуправлении односторонним контролем доступа оборудовано четыре кабинета, доступ в которые осуществляется через двери «Дверь ЗУ каб. 101», «Дверь ЗУ каб. 102», «Дверь ЗУ каб. 106», «Дверь ЗУ каб. 107».

На территории южного филиала находится склад, доступ в который осуществляется через дверь «Склад ЮФ».

К серверу оборудования через локальную сеть предприятия подключено оборудование СКУД Elsys в составе:

- два контроллера Elsys-MB-Standard, установленные на центральной проходной, подключенные через КСК Elsys-MB-Net № 1;
- два контроллера Elsys-MB-Standard и контроллер Elsys-MB-SM, установленные в южном филиале, подключенные через КСК Elsys-MB-Net № 2;
- три контроллера Elsys-MB-IP, установленные в заводоуправлении.

При настройке оборудования необходимо включить контроллеры Elsys-MB-IP в одну сетевую группу, введя в её состав также КСК Elsys-MB-Net № 1 (рисунок 104).

Затем, выбрав узел **«Коммуникационные контроллеры»**, для включения глобального контроля последовательности прохода нажать кнопку **«Включить во всех КСК»** (рисунок 105).

После выхода из конфигуратора автоматически запустится инициализация, после выполнения которой во всей системе будет включен глобальный контроль последовательности прохода.

Затем следует выполнить настройку областей контроля. Как видно из рисунка (рисунок 103), территорию предприятия можно разбить на пять областей контроля:

- «Вне территории»;
- «Территория предприятия»;
- «Южный филиал»;
- «Заводоуправление»;
- «Склад ЮФ».

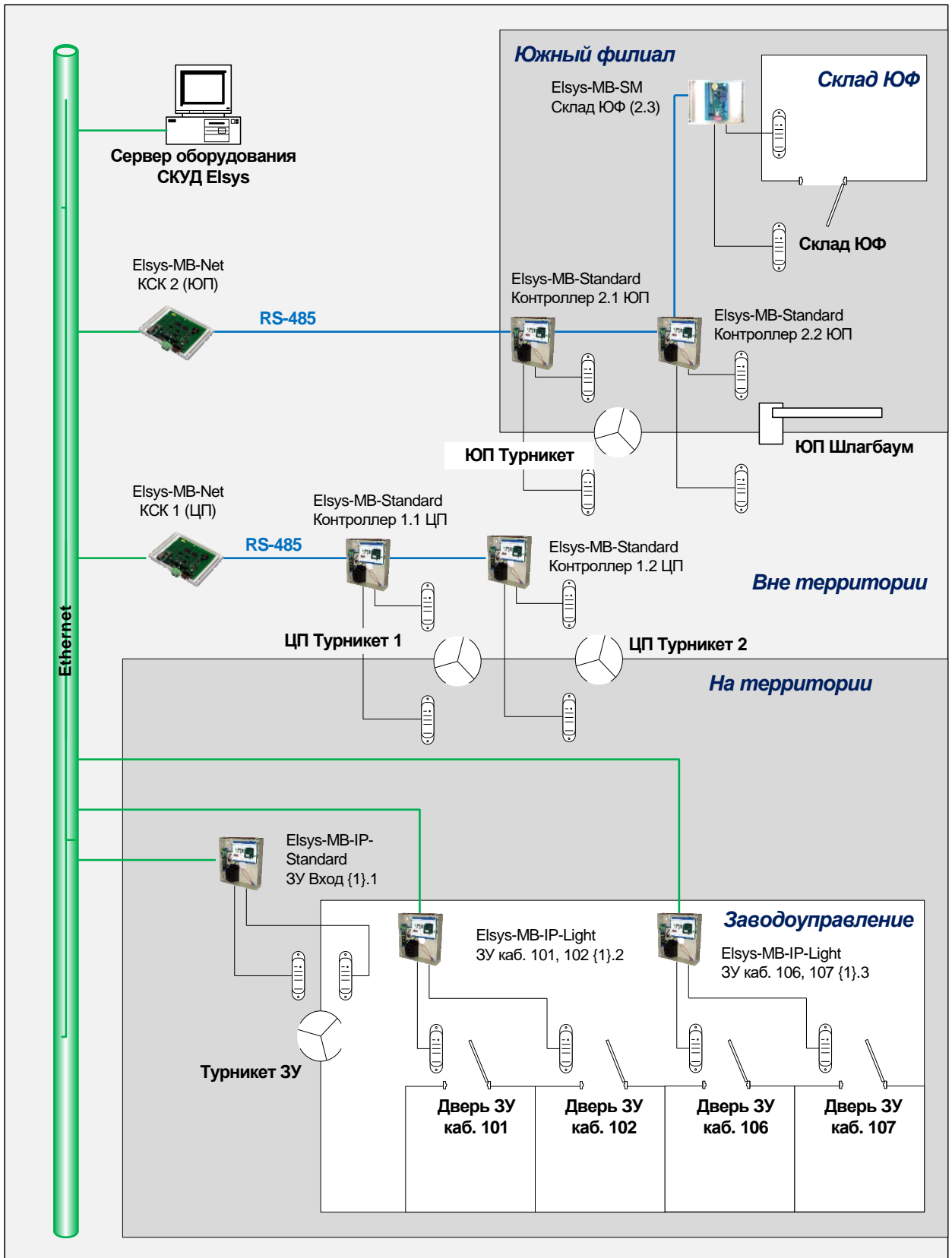


Рисунок 103 – Схема предприятия (пример настройки глобального контроля последовательности прохода)

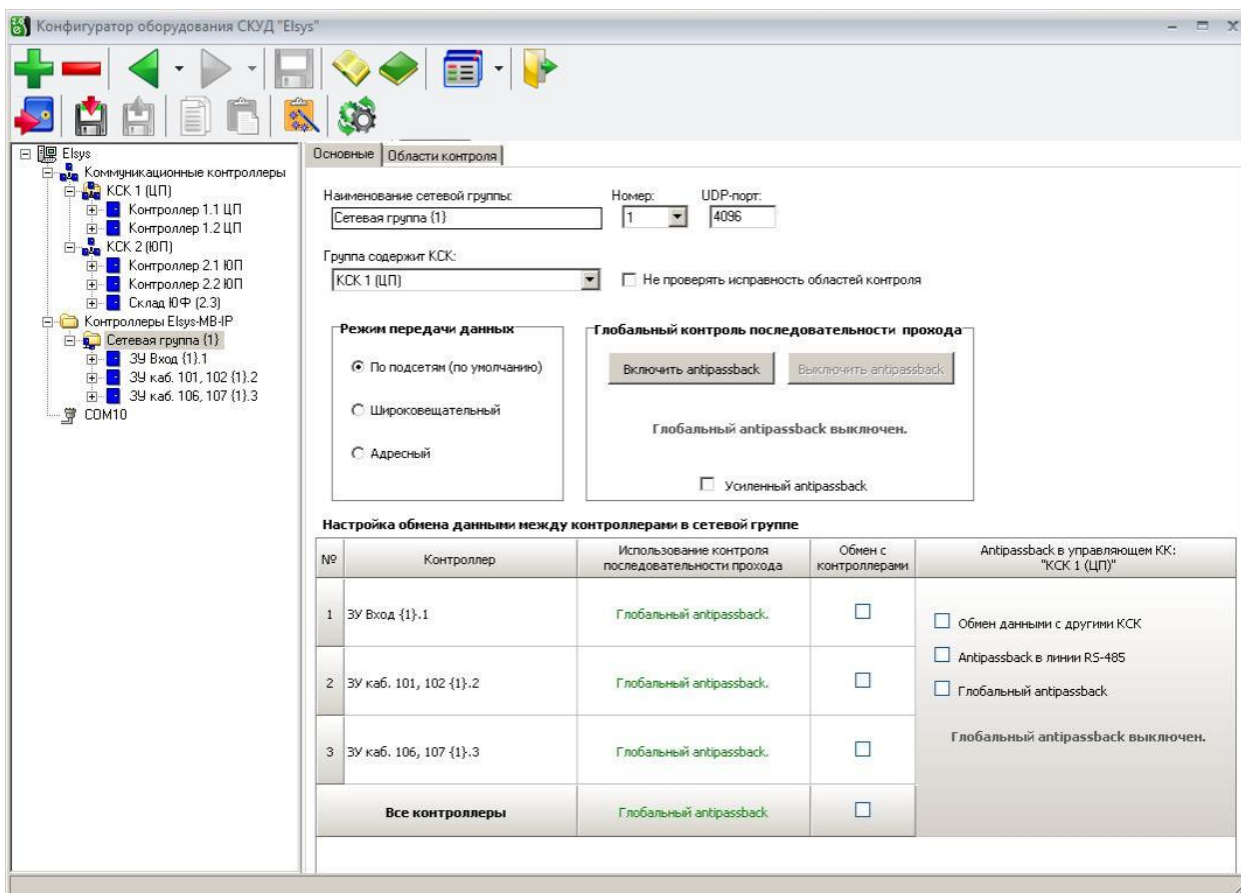


Рисунок 104 – Настройка сетевых групп для участия в едином информационном пространстве

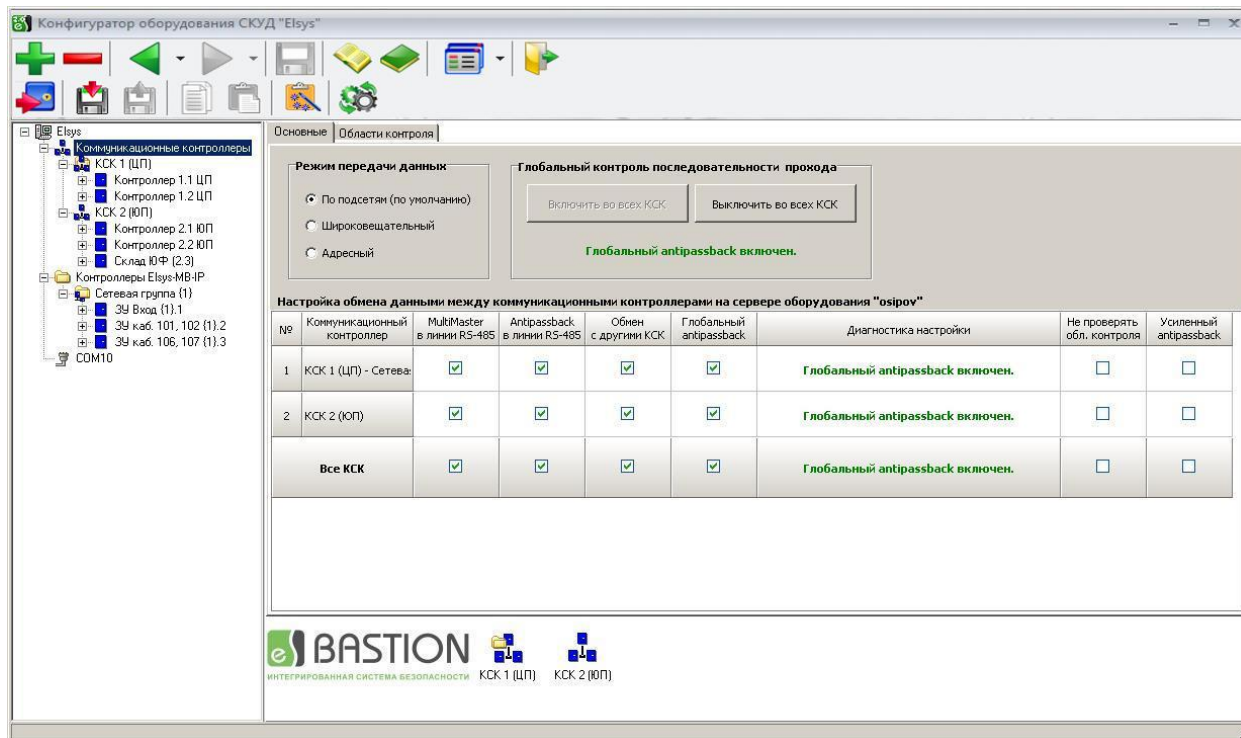


Рисунок 105 – Включение глобального контроля последовательности прохода

На рисунке 94 показано, как следует выполнить настройку областей контроля для данного объекта.

Следует обратить внимание, что для односторонних точек доступа, находящихся внутри заводоуправления, одна и та же область контроля – «Заводоуправление» – задана в качестве входной и выходной. Если сотрудник не попал штатным образом в заводоуправление, он не сможет получить доступ в кабинеты, находящиеся на его территории.

По окончании настройки областей контроля запустится автоматическая инициализация, после выполнения которой система готова к работе.

Убедиться в корректности настройки глобального контроля последовательности прохода можно в конфигураторе на странице свойств «Области контроля» в свойствах узла «Коммуникационные контроллеры» (рисунок 95).

## 7 Инициализация и управление контроллерами


**Внимание!** С настоящим разделом должны быть ознакомлены все, кто имеет отношение к эксплуатации, настройке и обслуживанию встроенного в ПО «Бастион-2» программного обеспечения «Бюро пропусков».

### 7.1 Инициализация контроллеров

Для загрузки данных в контроллеры необходимо провести инициализацию контроллеров. Инициализация может быть выполнена с любого компьютера в сети комплекса «Бастион-2» оператором, имеющим необходимые полномочия. В зависимости от полномочий пользователя ряд опций инициализации может быть запрещён.

Перед запуском системы в эксплуатацию необходимо проинициализировать полностью (со всеми включенными опциями) все контроллеры. В дальнейшем все изменения в базе данных, относящиеся к компетенции бюро пропусков (база данных персонала, уровни доступа, временные зоны, праздники) будут загружаться в контроллеры автоматически, при этом инициализация не требуется.

Если при передаче изменений в оборудование возникнут ошибки связи, об этом будет сообщено изменением цвета значка драйвера на панели драйвера «Бастион-2 – Elsys». Более подробную информацию (скорость обмена, выявленные ошибки, режим работы) можно получить, подведя мышь к значку драйвера или сетевого контроллера на панели управления драйвером «Бастион-2 – Elsys» (рисунок **Ошибка! Источник ссылки не найден.**).

Инициализация контроллеров вызывается с помощью кнопки **«Инициализация оборудования...»**, расположенной на ленте управления драйвером (рисунок 2). Также вызвать окно «Инициализация оборудования» можно из окна конфигуратора оборудования, нажав кнопку  на панели дополнительных средств драйвера.

В окне инициализации (рисунок 106) отображаются все контроллеры СКУД Elsys с учётом настроек отображения.



Назначение элементов на панели управления окна инициализации представлено в таблице 14.

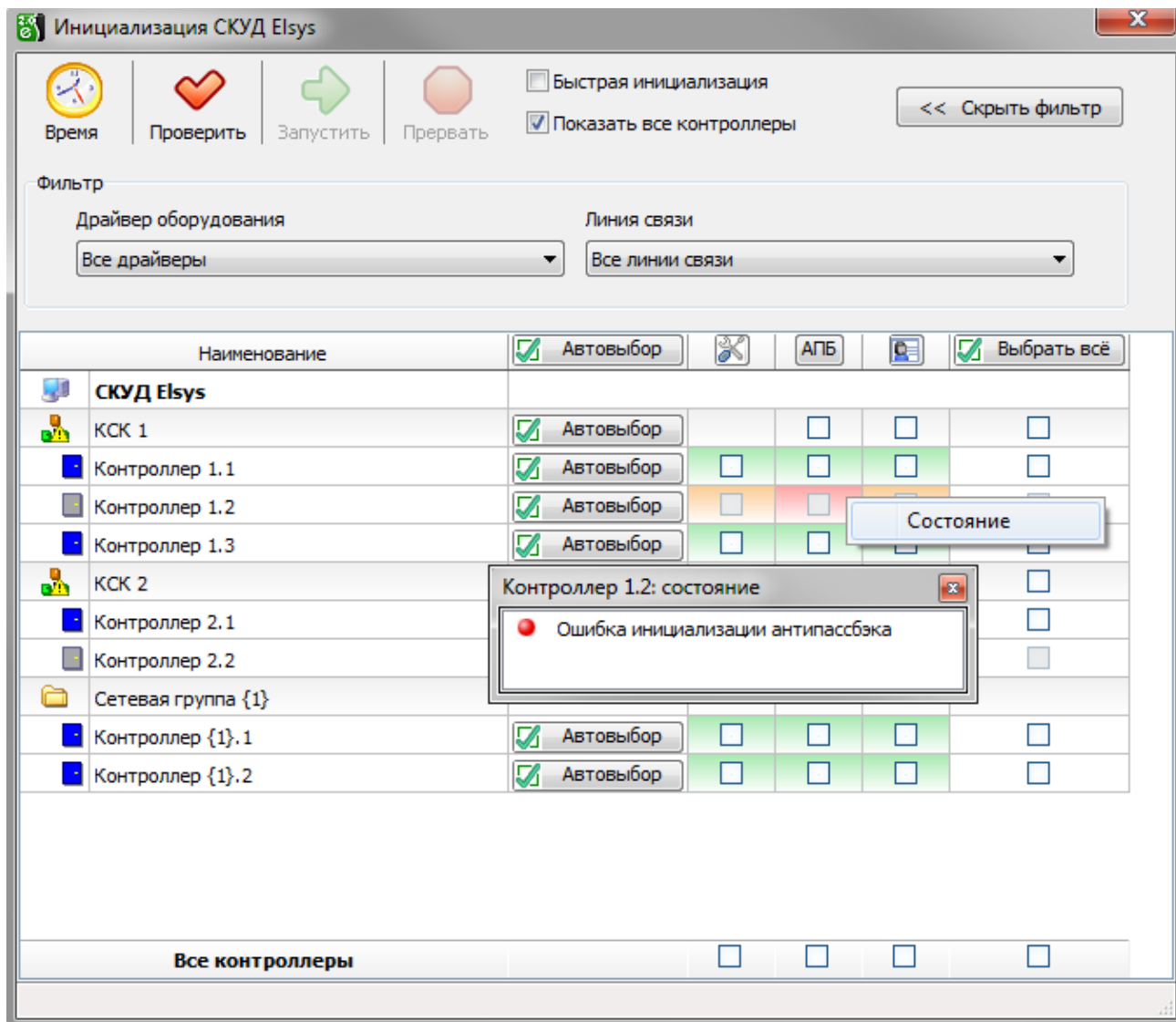


Рисунок 106 - Окно инициализации оборудования


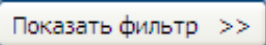
Список контроллеров представлен в табличном виде с возможностью фильтрации по драйверу оборудования и по линии связи.

По умолчанию, настройки фильтра скрыты, а в таблице отображаются только «проблемные контроллеры» - для которых есть какие-либо ошибки (ошибки инициализации, рассинхронизация в картах, отсутствует связь и др.) с выбранными требуемыми опциями инициализации.

Опция «Показать все контроллеры» включает отображение всех контроллеров СКУД Elsys.



Таблица 14 - Назначение элементов на панели управления окна инициализации

Элемент управления	Назначение
 Время	Кнопка служит для выполнения синхронизации даты и времени во всех контроллерах системы СКУД «Elsys», с которыми установлена связь.
 Проверить	Кнопка служит для запуска проверки конфигурации контроллеров. Проверка конфигурации запускается автоматически при открытии окна инициализации, а также после завершения инициализации. Результаты проверки конфигурации можно определить по цвету фона ячеек таблицы, а также из контекстного меню «Состояние» (рисунок 106).
 Запустить	Кнопка служит для запуска инициализации контроллеров, у которых установлены параметры инициализации.
 Прервать	Кнопка служит для прерывания процесса инициализации.
	Кнопка служит для отображения настроек фильтра контроллеров по серверам и драйверам оборудования, а также по линиям связи.
	Кнопка служит для скрытия настроек фильтра контроллеров.
<input type="checkbox"/> Быстрая инициализация	Опция позволяет отключить опрос контроллеров на время инициализации, что ускоряет процесс инициализации.
<input type="checkbox"/> Показать все контроллеры	Опция управляет отображением контроллеров в таблице. При включенной опции в таблице отображаются все контроллеры доступа СКУД Elsys в соответствии с настройками фильтра. При выключенной опции при отображении контроллеров также используются настройки фильтра, однако в таблице отображаются только контроллеры, у которых есть ошибки инициализации, ошибки в конфигурации, а также для которых требуется выполнить инициализацию по каким-либо причинам.

Если все параметры инициализации контроллеров в норме, то при открытии окна инициализации в таблице отображаются все контроллеры СКУД Elsys.

В первом столбце таблицы отображаются состояния контроллеров и линий связи. Описание возможных состояний представлено в таблице 15.

Кнопки в заголовке таблицы служат для быстрого выбора требуемых параметров инициализации контроллеров.

Таблица 15 - Описание возможных состояний контроллеров и линий связи



















Пиктограмма	Описание состояния
	Состояние COM-порта неизвестно
	COM-порт отсутствует или используется другим приложением
	Включен режим обмена MASTER-SLAVE на COM-порту (выключен глобальный контроль последовательности прохода)
	Отсутствует связь с одним или несколькими контроллерами в режиме MASTER-SLAVE на COM-порту
	Идет инициализация в режиме MASTER-SLAVE на COM-порту
	Есть ошибки инициализации в режим MASTER-SLAVE на COM-порту
	Включен режим обмена MULTIMASTER на COM-порту (включен глобальный контроль последовательности прохода)
	Отсутствует связь с одним или несколькими контроллерами в режиме MULTIMASTER на COM-порту
	Идет инициализация в режиме MULTIMASTER на COM-порту
	Есть ошибки инициализации в режиме MULTIMASTER на COM-порту
	Состояние сетевого контроллера неизвестно
	Состояние сетевого контроллера, входящего в сетевую группу, неизвестно.
	Отсутствует соединение с сетевым контроллером
	Отсутствует соединение с сетевым контроллером, входящим в сетевую группу.
	Включен режим обмена MASTER-SLAVE на сетевом контроллере (выключен глобальный контроль последовательности прохода)
	Включен режим обмена MASTER-SLAVE на сетевом контроллере, входящим в сетевую группу (выключен глобальный контроль последовательности прохода)
	Отсутствует связь с одним или несколькими контроллерами в режиме MASTER-SLAVE на сетевом контроллере
	Отсутствует связь с одним или несколькими контроллерами в режиме MASTER-SLAVE на сетевом контроллере, входящим в сетевую группу

Таблица 15 - Описание возможных состояний контроллеров и линий связи














Пиктограмма	Описание состояния
	Идет инициализация в режиме MASTER-SLAVE на сетевом контроллере
	Идет инициализация в режиме MASTER-SLAVE на сетевом контроллере, входящим в сетевую группу
	Есть ошибки инициализации в режиме MASTER-SLAVE на сетевом контроллере
	Есть ошибки инициализации в режиме MASTER-SLAVE на сетевом контроллере, входящим в сетевую группу
	Включен режим обмена MULTIMASTER на сетевом контроллере (включен глобальный контроль последовательности прохода)
	Включен режим обмена MULTIMASTER на сетевом контроллере, входящим в сетевую группу (включен глобальный контроль последовательности прохода)
	Отсутствует связь с одним или несколькими контроллерами в режиме MULTIMASTER на сетевом контроллере
	Отсутствует связь с одним или несколькими контроллерами в режиме MULTIMASTER на сетевом контроллере, входящим в сетевую группу
	Идет инициализация в режиме MULTIMASTER на сетевом контроллере
	Идет инициализация в режиме MULTIMASTER на сетевом контроллере, входящим в сетевую группу
	Есть ошибки инициализации в режиме MULTIMASTER на сетевом контроллере
	Есть ошибки инициализации в режиме MULTIMASTER на сетевом контроллере, входящим в сетевую группу
	Состояние контроллеров в сетевой группе неизвестно
	Связь со всеми контроллерами Elsys-MB-IP в сетевой группе в норме
	Отсутствует связь как минимум с одним контроллером Elsys-MB-IP в сетевой группе
	Идет инициализация контроллеров Elsys-MB-IP в сетевой группе
	Есть ошибки инициализации контроллеров Elsys-MB-IP в сетевой группе

Таблица 15 - Описание возможных состояний контроллеров и линий связи


Пиктограмма	Описание состояния
	Состояние контроллеров в сетевой группе неизвестно, сетевая группа включает сетевой контроллер
	Связь со всеми контроллерами Elsys-MB-IP в сетевой группе в норме, сетевая группа включает сетевой контроллер
	Отсутствует связь как минимум с одним контроллером Elsys-MB-IP в сетевой группе, сетевая группа включает сетевой контроллер
	Идет инициализация контроллеров Elsys-MB-IP в сетевой группе, сетевая группа включает сетевой контроллер
	Есть ошибки инициализации контроллеров Elsys-MB-IP в сетевой группе, сетевая группа включает сетевой контроллер



В строках таблицы для каждого контроллера можно указать параметры инициализации индивидуально: инициализацию оборудования, антипассбэка или карт доступа.

Контроллеры и линии связи, с которыми отсутствует связь, отображаются серым цветом и не доступны для инициализации.

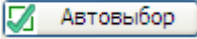

Состояние каждого параметра инициализации можно определить по цвету в ячейке таблицы и детально из контекстного меню **«Состояние»** (рисунок 106).

Если фон ячейки таблицы какого-либо параметра инициализации имеет зеленый цвет, то выполнять инициализацию этого параметра не требуется. Красный цвет ячейки показывает наличие ошибок в процессе инициализации. Оранжевым цветом отображаются параметры инициализации контроллеров, у которых были выявлены ошибки в процессе проверки конфигурации, или которые требуется проинициализировать. Чёрным цветом отображаются ошибки в конфигурации контроллеров, которые не устраняются инициализацией - превышение допустимого количества карт и т.п.

Кнопка  **Автовыбор** служит для выбора требуемых параметров инициализации. При нажатии на кнопку в заголовке таблицы для всех контроллеров в таблице выбираются все параметры инициализации, которые имеют какие-либо ошибки (отображаются не зеленым цветом). При нажатии на кнопку внутри таблицы выбираются требуемые параметры инициализации конкретного контроллера.

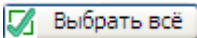
Кнопки  **АПБ** и  служат для выбора конкретных параметров инициализации: инициализации оборудования, антипассбэка или карт доступа, при наличии каких-либо ошибок в этих параметрах.

Например, инициализацию оборудования следует проводить после начальной настройки системы и внесения изменений в настройку оборудования. Во втором случае достаточно проинициализировать лишь те контроллеры, в конфигурацию которых были внесены изменения. Параметры инициализации оборудования таких контроллеров отображаются

оранжевым цветом фона ячеек таблицы и автоматически выбираются при открытии окна инициализации, а также при нажатии на кнопку  **Автовыбор** или .

**Внимание!** Если в процессе настройки добавлялись контроллеры, добавлялись или удалялись двери, считыватели, турникеты, или изменялось распределение памяти контроллеров, необходимо полностью проинициализировать все контроллеры.

Инициализацию антипассбэка следует проводить во всех контроллерах, если вносились изменения в конфигурацию областей контроля, а также при начальной настройке системы. В конфигураторе оборудования выполняется отслеживание этих изменений и, если требуется, инициализация антипассбэка запускается автоматически при закрытии окна конфигуратора оборудования.

Кнопка  **Выбрать всё** служит для выбора всех параметров инициализации в таблице.

Выбор параметров инициализации отдельных контроллеров осуществляется щелчком мыши в ячейках, соответствующих требуемым параметрам.

Элементы управления в нижнем колонтитуле таблицы и в крайнем правом столбце используются для выбора или отмены выбора параметров инициализации соответственно по строками и столбцам.

Назначение элементов на панели управления окна инициализации представлено в таблице 14.

**Внимание!** Следует учитывать, что в процессе инициализации оборудование может работать неверно. Так, при инициализации списка карт доступа сначала полностью очищается список карт контроллера, а затем по одной заносятся новые карты. Соответственно, карты доступа, которые в текущий момент времени ещё не проинициализированы, будут опознаваться как «Неизвестная карта».

## 7.2 Управление контроллерами

Функции управления контроллерами доступны из контекстного меню в столбце с наименованиями контроллеров (рисунки 107 - 108 ).

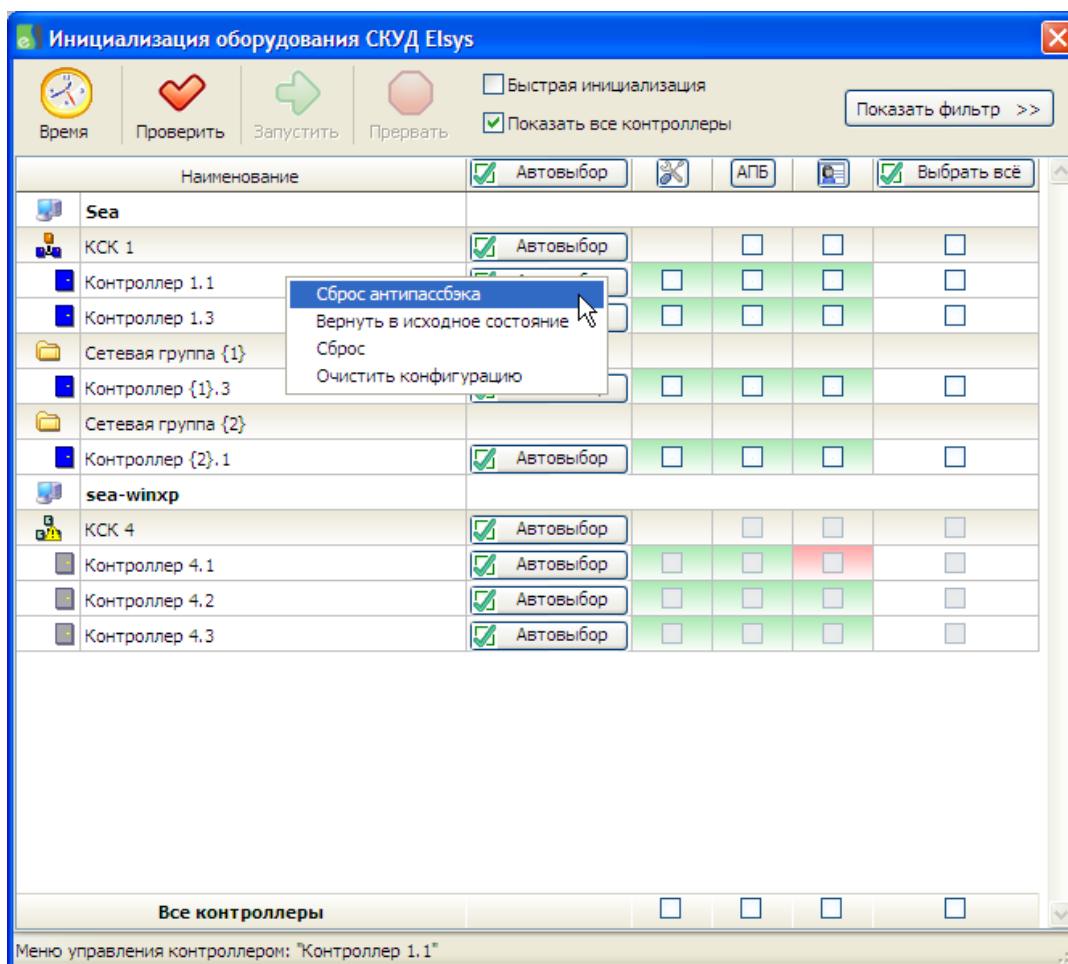


Рисунок 107 - Управление контроллером доступа из окна инициализации

Команда «Сброс антипассбэка» сбрасывает информацию о текущей зоне доступа всех пользователей в выбранном контроллере.

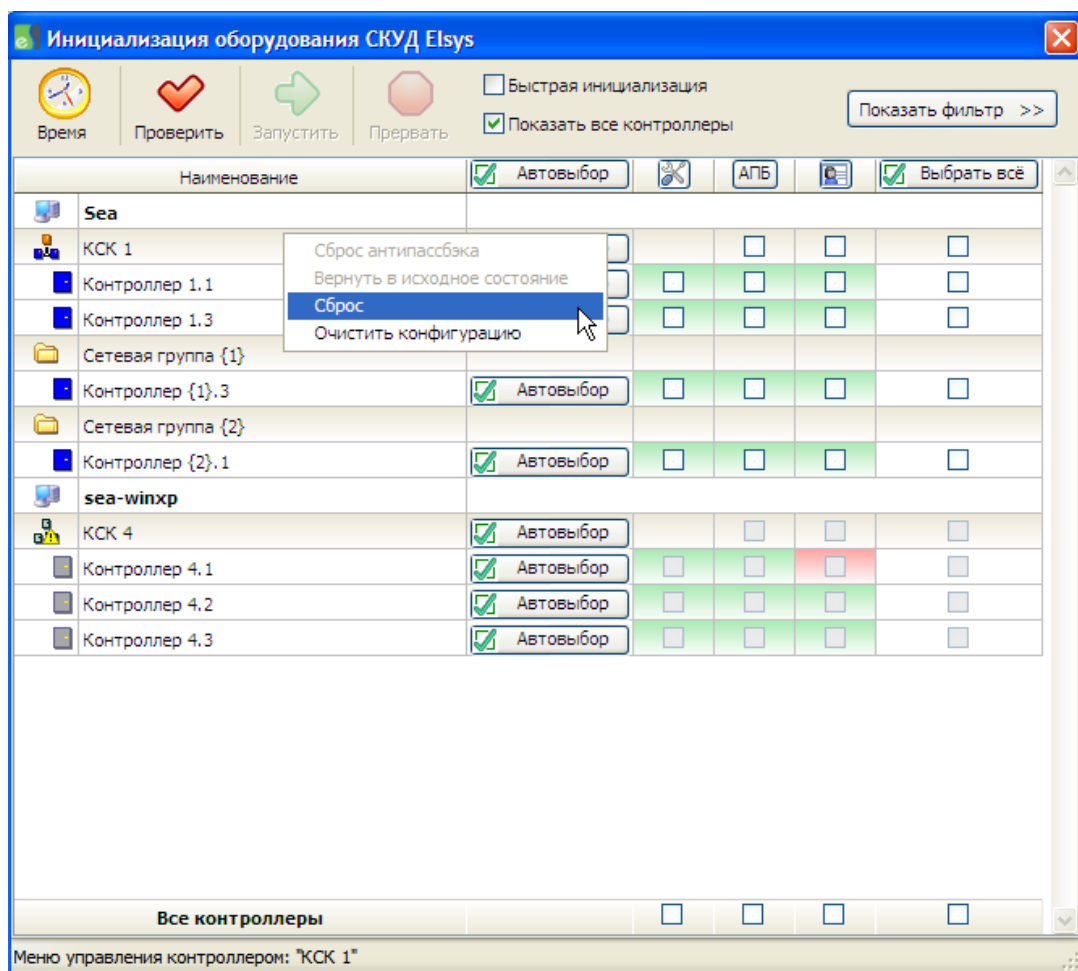


Рисунок 108 - Управление сетевым контроллером из окна инициализации

Команда **«Вернуть в исходное состояние»** возвращает в нормальное состояние все устройства в составе контроллера (Входы – вне охраны, точки прохода – в нормальный режим, выходы – выключены) и может использоваться, если состояние ряда устройств неизвестно.

Команда **«Сброс»** выполняет перезапуск встроенного ПО выбранного контроллера аналогично кнопке «RESET» на плате контроллера.

Команда **«Очистить конфигурацию»** полностью очищает конфигурацию выбранного контроллера, что эквивалентно аппаратной очистке конфигурации (кнопками CLEAR и RESET на плате контроллера), за исключением того, что не изменяется адрес и скорость обмена контроллера доступа. Для сетевых контроллеров конфигурация устанавливается по умолчанию (IP-адрес - 192.168.127.254 и номер 4040).

### 7.3 Восстановление протокола событий

Для контроллеров доступа с версией прошивки 2.60 и выше существует возможность прочитать события из контроллера за указанный интервал времени (восстановить протокол событий), если произошел сбой с потерей данных (рисунок 109).

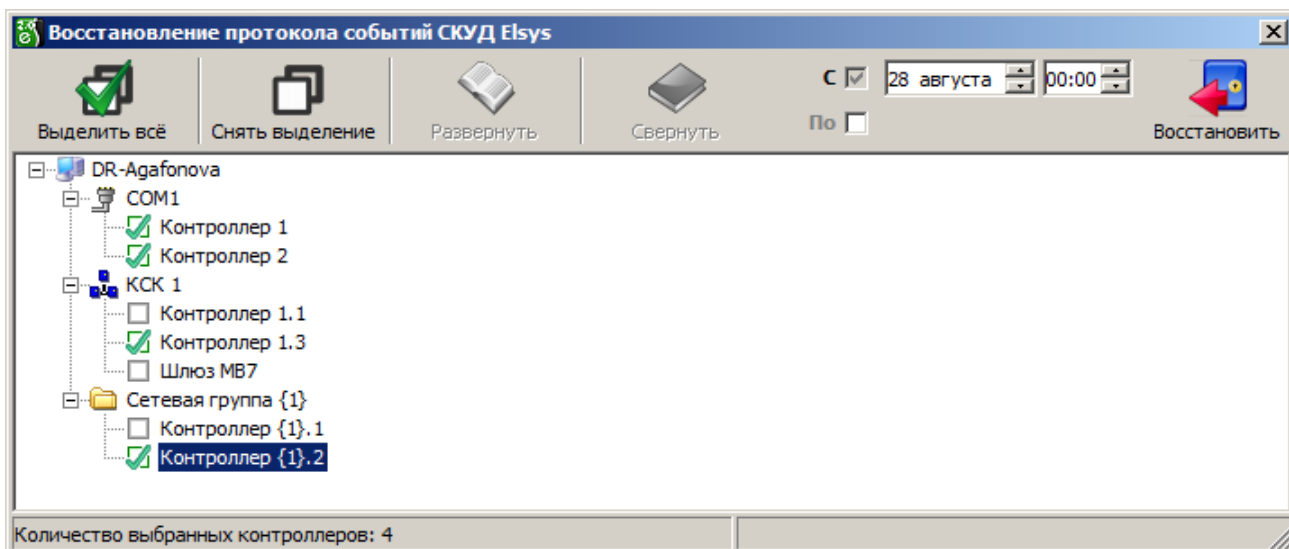


Рисунок 109 – Восстановление буфера событий

**Внимание!** Восстановление протокола событий – длительная операция, которая приводит к большой загрузке системы и может на некоторое время нарушить ее нормальную работу.

Режим восстановления протокола событий запускается с помощью кнопки «Восстановление протокола событий», расположенной на ленте управления драйвером.

Для восстановления протокола событий следует выбрать все контроллеры доступа, события от которых следует восстановить, задать период времени и нажать кнопку «Восстановить».

При указании периода времени обязательным является задание начальной даты. Для задания даты и времени окончания периода следует установить опцию «По» и задать требуемые значения. Если указано только начало периода, то будут восстановлены все события с начала указанного периода времени.

При успешном восстановлении протокола событий будет сформировано событие контроллера «Восстановление буфера событий».

При частичном восстановлении протокола событий будет сформировано событие «Частичное восстановление буфера событий».

**Внимание!** Для корректной работы функции восстановления протокола событий должны быть выполнены следующие условия:

- 1) дата конца периода не должна превышать текущей даты (время может быть до 23:59 от текущей даты);
- 2) если текущий месяц находится в диапазоне с января по ноябрь, то допустимо указать месяц начала периода - декабрь, при этом будет считаться, что это предыдущий год;
- 3) если текущий месяц - декабрь, то месяц начала периода допустимо задавать в диапазоне с января по декабрь, при этом будет считаться, что это текущий год;



4) дата начала периода не должна превышать дату конца периода (кроме п. 2, где считается, что это предыдущий год).

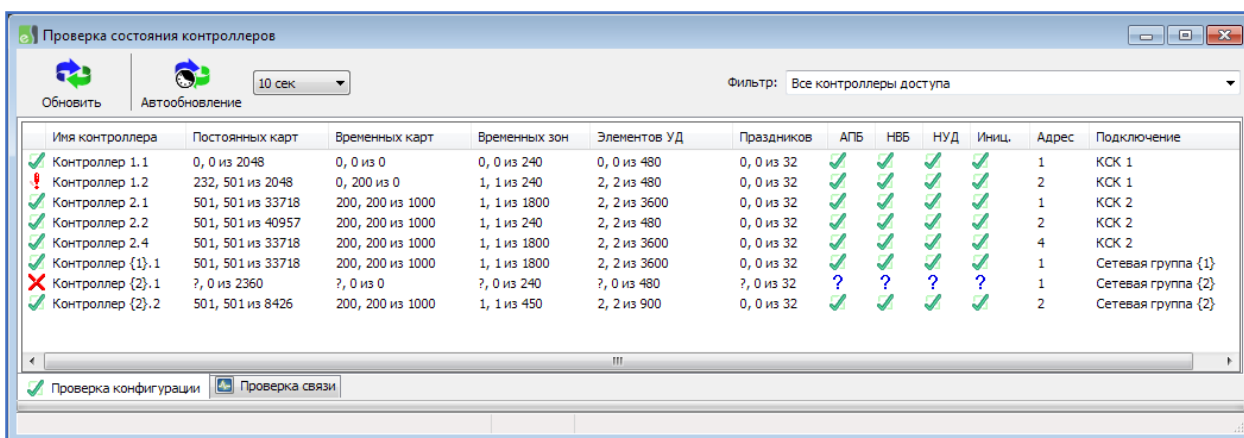
## 8 Проверка текущего состояния контроллеров

### 8.1 Проверка конфигурации контроллеров

При необходимости можно проверить конфигурацию контроллеров доступа (число карт, уровней доступа, временных интервалов и т. д.).

Окно проверки конфигурации контроллеров вызывается с помощью кнопки «**Проверка конфигурации**», расположенной на ленте управления драйвером (рисунок 2).

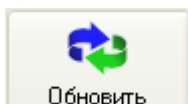
Окно проверки конфигурации контроллеров показано на рисунке (рисунок 110).



Имя контроллера	Постоянных карт	Временных карт	Временных зон	Элементов УД	Праздников	АПБ	НВБ	НУД	Иниц.	Адрес	Подключение
Контроллер 1.1	0, 0 из 2048	0, 0 из 0	0, 0 из 240	0, 0 из 480	0, 0 из 32	✓	✓	✓	✓	1	КСК 1
Контроллер 1.2	232, 501 из 2048	0, 200 из 0	1, 1 из 240	2, 2 из 480	0, 0 из 32	✓	✓	✓	✓	2	КСК 1
Контроллер 2.1	501, 501 из 33718	200, 200 из 1000	1, 1 из 1800	2, 2 из 3600	0, 0 из 32	✓	✓	✓	✓	1	КСК 2
Контроллер 2.2	501, 501 из 40957	200, 200 из 1000	1, 1 из 240	2, 2 из 480	0, 0 из 32	✓	✓	✓	✓	2	КСК 2
Контроллер 2.4	501, 501 из 33718	200, 200 из 1000	1, 1 из 1800	2, 2 из 3600	0, 0 из 32	✓	✓	✓	✓	4	КСК 2
Контроллер {1}.1	501, 501 из 33718	200, 200 из 1000	1, 1 из 1800	2, 2 из 3600	0, 0 из 32	✓	✓	✓	✓	1	Сетевая группа {1}
Контроллер {2}.1	?, 0 из 2360	?, 0 из 0	?, 0 из 240	?, 0 из 480	?, 0 из 32	?	?	?	?	1	Сетевая группа {2}
Контроллер {2}.2	501, 501 из 8426	200, 200 из 1000	1, 1 из 450	2, 2 из 900	0, 0 из 32	✓	✓	✓	✓	2	Сетевая группа {2}

Рисунок 110 - Отчёт по конфигурации контроллеров

При создании окна всем контроллерам доступа посылается запрос, в ответ на который контроллеры сообщают свои количественные характеристики (количество временных зон, уровней доступа, праздников, карт).



Кнопка **Обновить** запускает процесс повторного опроса контроллеров и обновления показаний.



Кнопка **Автообновление** включает автоматическое обновление показаний через заданный интервал времени, который выбирается в выпадающем списке справа от кнопки. Доступные интервалы обновления — 0,5 сек, 1 сек, 5 сек, 10 сек, 30 сек и 1 минута.

Список контроллеров может быть отфильтрован по типу подключения контроллера доступа (рисунок 111):

- все контроллеры доступа, подключенные через COM-порт;
- все контроллеры доступа, подключенные через КСК;

- все контроллеры Elsys-MB-IP.

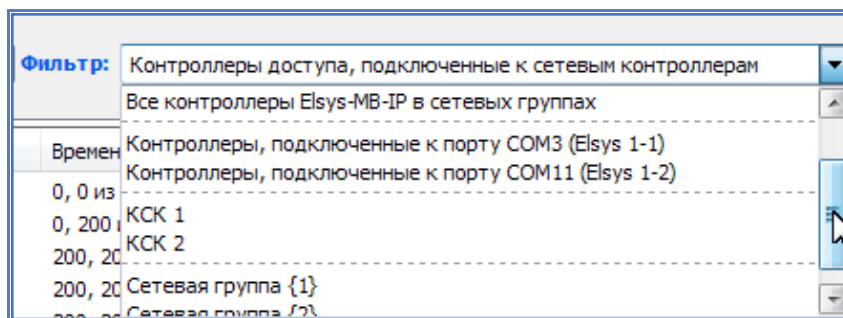





Рисунок 111 - Фильтр по подключению в окне проверки конфигурации

Фильтр позволяет также получить список контроллеров доступа, подключенных к конкретному КСК, COM-порту или входящих в выбранную сетевую группу.

Данные по всем контроллерам выводятся в виде таблицы.

Первая колонка – рисунок, отражающий состояние контроллера. Значок  означает отсутствие ошибок в конфигурации контроллера, значок  указывает на наличие ошибок в конфигурации, значок  означает отсутствие связи с контроллером в момент запроса конфигурации.

Колонка **«Имя контроллера»** – наименование контроллера из базы данных.

В каждой из колонок **«Постоянных карт»**, **«Временных карт»**, **«Временных зон»**, **«Уровней доступа»**, **«Праздников»** содержатся три значения. Первое значение – количественная характеристика, сообщённая контроллером; второе значение – количественная характеристика, взятая из базы данных; третье значение – максимально возможное для данного контроллера (зависит от варианта исполнения, версии, и ряда настроек).

Контроллеры версий ниже 1.34 не сообщают свои количественные характеристики, поэтому для них первая цифра будет отсутствовать.



Колонка **«Постоянных карт»** показывает число постоянных карт.



Колонка **«Временных карт»** показывает число временных карт.



Колонка **«Временных зон»** показывает число временных зон.



Колонка **«Уровней доступа»** показывает число уровней доступа.

Колонка **«Праздников»** показывает число праздников.

Колонка **«АПБ»** показывает состояние конфигурации областей контроля: значок  означает отсутствие ошибок, значок  указывает на наличие ошибок в конфигурации.

Колонка **«НВБ»** показывает состояние нумерации временных блоков: значок  означает отсутствие ошибок, значок  указывает на наличие ошибок в конфигурации.

Колонка **«НУД»** показывает состояние нумерации уровней доступа: значок  означает отсутствие ошибок, значок  указывает на наличие ошибок в конфигурации.

Колонка **«Иниц.»** показывает наличие ошибок инициализации (в том числе автоматической загрузки данных, происходящей при добавлении/удалении карт в бюро пропусков, редактировании уровней доступа и временных блоков): значок  означает отсутствие ошибок инициализации, значок  указывает на наличие ошибок инициализации.

Колонка **«Адрес»** показывает адрес контроллера.

Колонка **«Подключение»** показывает, каким образом подключен контроллер – через СОМ-порт, сетевой контроллер или входит в сетевую группу.

Колонка **«Вер. Elsys-MB»** показывает номер версии встроенного программного обеспечения контроллера.

Колонка **«Вер. Elsys-IP»** показывает номер версии встроенного программного обеспечения интерфейсного Ethernet-модуля Elsys-MB-IP.

Колонка **«Вариант исп.»** показывает вариант исполнения контроллера.

Колонка **«МРП»** показывает тип модуля расширения памяти в контроллере при его наличии.

Если были обнаружены ошибки в конфигурации контроллеров, необходимо проинициализировать все контроллеры. Ошибки возможны, если по ряду причин не все изменения были переданы в контроллеры. Ошибки могут быть вызваны также неверным заданием версии прибора, заданием двух полностью идентичных временных зон, относящихся к одному блоку (контроллер проверяет уникальность временных зон и не добавит их дважды).

## 8.2 Проверка наличия связи с контроллерами

Окно проверки конфигурации контроллеров вызывается с помощью кнопки **«Проверка конфигурации»**, расположенной на ленте управления драйвером (рисунок 2) и последующим переходом на вкладку «проверка связи».

Окно проверки связи показано на рисунке 112.

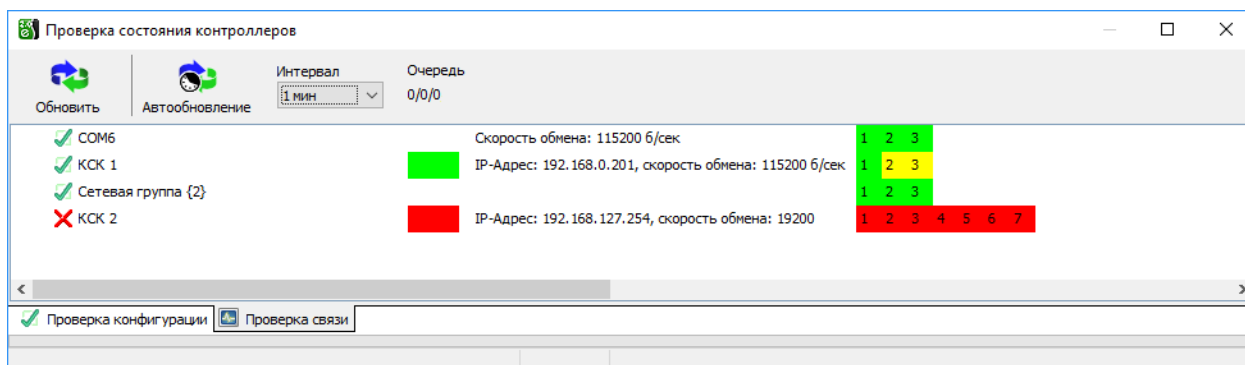




Рисунок 112 - Окно проверки связи с контроллерами

В первой колонке отображается состояние линии связи (сетевой группы, КСК). Наличие связи с драйвером отображается знаком , отсутствие связи с КСК – знаком  и отсутствие связи с драйвером – знаком вопроса.

В третьей колонке зелёным или красным прямоугольником отображается соответственно наличие и отсутствие связи с КСК.

В правой части зелёными, желтыми или красными прямоугольниками отображается состояние связи с контроллерами и результат проверки конфигурации.

Зелёный – связь есть, ошибок конфигурации не обнаружено.

Жёлтый – связь есть, присутствуют ошибки или расхождения в конфигурации или идёт процесс доставки изменений в контроллер.

Красный – нет связи с контроллером.

***Внимание!** Во время загрузки драйвера и первоначального опроса конфигурации контроллеров, в окне проверки связи отображается отсутствие связи с КСК и контроллерами. Окончание процесса загрузки и опроса можно определить по обновлению поля «Очередь» с «Неизвестно» на «0/0/0»*

В поле «Очередь» отображается процесс загрузки изменений в контроллеры в виде трёх чисел – количество полученных изменений, количество обработанных изменений и количество ошибок (повторов).

При отсутствии ответа от драйвера отображается «Неизвестно».

## 9 Дополнительные сведения по настройке драйвера «Бастион-2 – Elsys»

### 9.1 Система программируемых аппаратных взаимодействий

Система программируемых аппаратных взаимодействий, имеющаяся в контроллерах Elsys-MB, предоставляет дополнительные возможности для самостоятельного программирования алгоритмов работы контроллера, что позволяет реализовывать специфические требования к системе управления доступом или использовать контроллеры вне рамок систем управления доступом, например, в системах управления зданием или в устройствах промышленной автоматике.

Принцип программирования и работы взаимодействий заключается в том, что на событие от какого-либо устройства назначается команда по управлению другим устройством. События и команды могут иметь дополнительные параметры. Взаимодействия (до 100 на контроллер) предварительно настраиваются в ПО «Бастион-2» и затем, при инициализации, загружаются в память контроллеров. В дальнейшем они выполняются встроенным программным обеспечением контроллера, **без участия компьютера**.

Следует различать аппаратные взаимодействия контроллеров Elsys-MB и аппарат реакций (реализуется программным способом через сценарии и реакции на события; описан в «Руководстве администратора»).

**Внимание!** Всегда, если необходимо организовать взаимодействие устройств, относящихся к одному контроллеру, следует использовать аппаратные взаимодействия, описанные в настоящей главе.

### 9.1.1 Настройка взаимодействий

Для настройки взаимодействий в дереве устройств следует выбрать узел «**Взаимодействия**» (рисунок 113), относящийся к настраиваемому контроллеру, после чего в правой части экрана появится страница свойств «**Взаимодействия**» (рисунок 114).

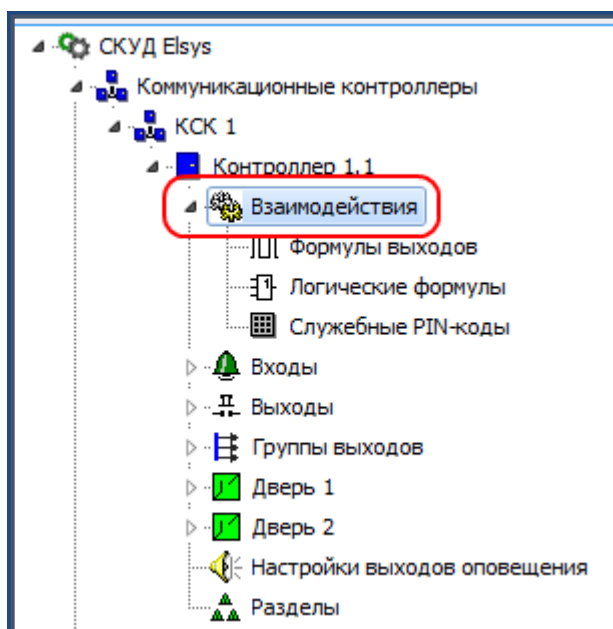


Рисунок 113 – Настройка взаимодействий

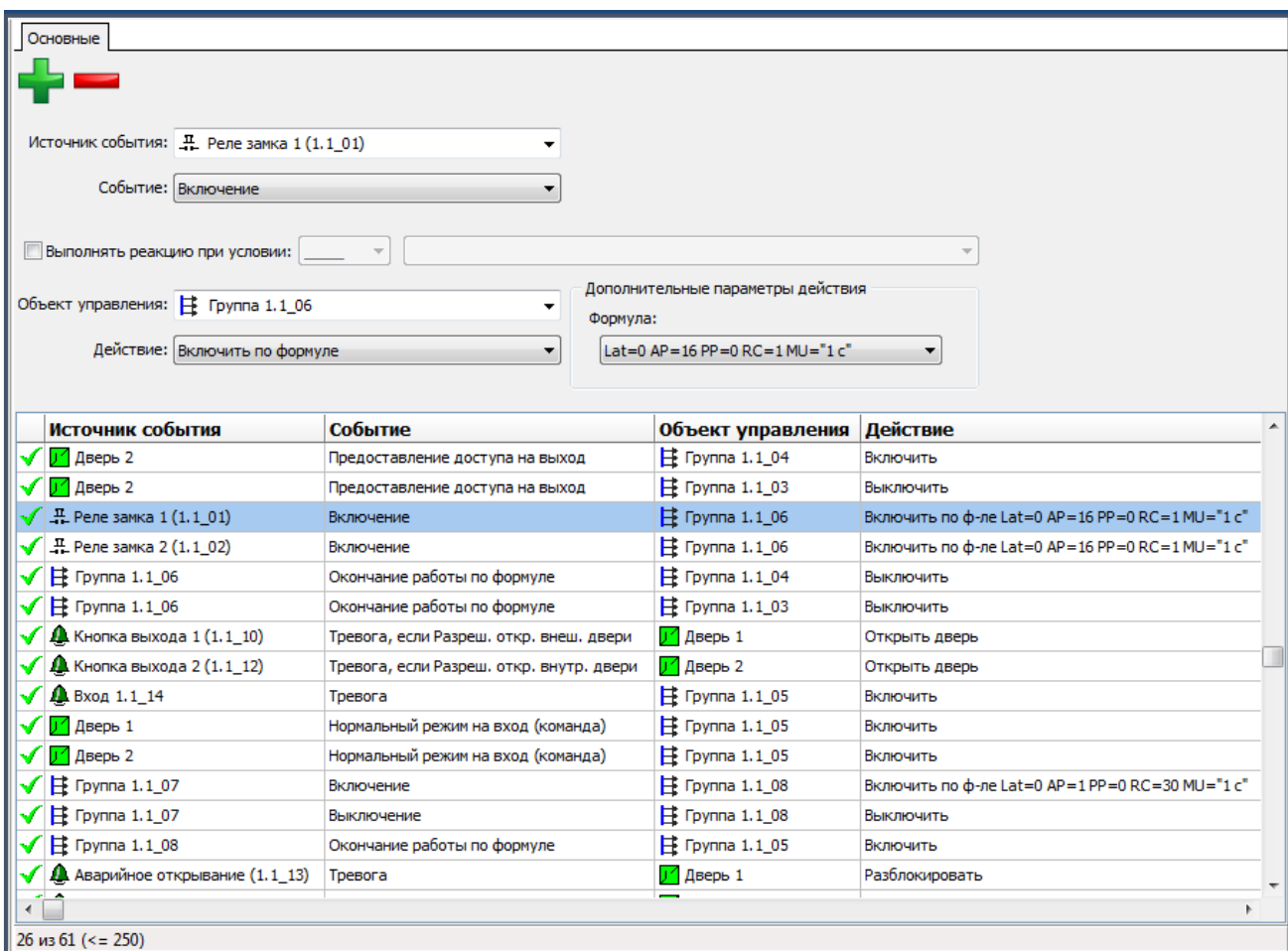


Рисунок 114 - Окно настройки взаимодействий



В нижней части окна все взаимодействия представлены в табличном виде (с помощью мыши или клавиатуры можно выбрать запись для редактирования), а в верхней части находятся элементы, с помощью которых можно добавить новое взаимодействие, выполнить редактирование или удалить существующее взаимодействие.

Назначение кнопок на странице взаимодействий приведено в таблице 16.

Таблица 16 - Панель инструментов окна редактирования взаимодействий

Кнопка	Назначение
	Добавляет новое взаимодействие.  После нажатия этой кнопки следует последовательно, сверху вниз заполнить списки выбора «Источник события», «Событие», «Объект управления», «Действие», и если необходимо, задать дополнительные параметры. Списки «Событие» и «Действие» зависят от типов устройств, выбранных в полях «Источник события» и «Объект управления».
	Удаляет выбранное взаимодействие.

Если события и управляющие действия имеют параметры (формула выхода, временной блок, время действия и др.), необходимые элементы редактирования контекстно отображаются в полях **«Дополнительные параметры события»**, **«Дополнительные параметры действия»**.

Если параметры события или команды заданы неверно, взаимодействие отображается в таблице значком  (такие взаимодействия не используются при загрузке данных в контроллеры), а если всё верно, значком .

Чтобы задать дополнительное условие для выполнения реакции на событие, следует включить опцию **«Выполнять реакцию при условии»** и выбрать нужную логическую формулу (см. п. 9.1.3) в качестве условия.



В базу данных все изменения во взаимодействиях записываются после нажатия кнопки **«Сохранить»** (таблица 2, п. 5) конфигуратора оборудования.

**Внимание!** Следует помнить, что для обеспечения логики работы точек доступа (двери, турникеты) не нужно настраивать взаимодействия (исключение составляют события-команды **«Разблокировать»**, **«Заблокировать»**, **«Нормальный режим»**).

### 9.1.2 Настройка формул управления работой выходов

Для редактирования списка формул управления работой выходов следует выбрать узел **«Формулы выходов»**, который является дочерним узла **«Взаимодействия»**, после чего в правой части экрана появится окно со страницей свойств **«Формулы выхода»** (рисунок 115).

Основные

Наименование:

Задержка:

Длительность активной части периода:  (0-98, 99 - постоянно)

Длительность пассивной части периода:  (0-98, 99 - постоянно)

Число повторений:  (0-98, 99 - всегда пульсировать)

Единица измерения:

Наименование	Задержка	Активная ч...	Пассивная ...	Количество ...	Ед. Изм.
Lat=0 AP=16 PP=0 RC=1 MU="1 c"	0	16	0	1	1 c
Lat=0 AP=2 PP=2 RC=99 MU="0,1 c"	0	2	2	99	0,1 c
Lat=0 AP=1 PP=0 RC=30 MU="1 c"	0	1	0	30	1 c
Lat=1 AP=99 PP=0 RC=1 MU="1 c"	1	99	0	1	1 c
Lat=0 AP=3 PP=0 RC=1 MU="1 c"	0	3	0	1	1 c
Lat=1 AP=1 PP=3 RC=30 MU="0,1 c"	1	1	3	30	0,1 c
Lat=0 AP=5 PP=5 RC=99 MU="0,1 c"	0	5	5	99	0,1 c

1 из 7 (<= 32)

Рисунок 115 - Окно настройки формул управления работой выходов

Для каждого контроллера Elsys-MB может быть задано до 16 формул, описывающих алгоритмы работы выходов контроллера, используемые во взаимодействиях – в команде **«Включить выход по формуле»**. Наименование формул не доступно для редактирования, формируется автоматически и содержит полную информацию о формуле в следующем формате:

**«Lat»** – задержка включения выхода,

**«AP»** – длительность активной части периода (выход включен),

**«PP»** – длительность пассивной части периода (выход выключен),

**«RC»** – число пульсаций,

**«MU»** – единица измерения времени для данной формулы. Допустимые единицы измерения – 0,1 с, 1 с, 10 с, 1 мин, 10 мин.

### 9.1.3 Логические формулы

Логическая формула – это логическое выражение, состоящее из последовательности логических условий, объединенных логическими операциями «И», «ИЛИ», «ИСКЛЮЧАЮЩЕЕ ИЛИ», «НЕ».

В качестве логических условий могут быть использованы состояния входов, выходов, групп выходов, временных блоков и логических формул (таблица 17).

Для редактирования списка логических формул следует выбрать узел **«Логические формулы»** узла **«Взаимодействия»**, после чего в правой части экрана появится окно, изображённое на рисунке (рисунок 116).

Пользовательский интерфейс составления логической формулы позволяет включать в одну формулу до трёх условий, однако использование в качестве операндов других логических формул позволяет составлять многоэлементные логические формулы.

Скобки в логическом выражении обеспечивают последовательное выполнение логических операций в порядке их расположения на фрейме (сверху вниз).

**Таблица 17 – Перечень состояний, используемых в логических формулах**

Тип операнда в логическом условии	Перечень состояний
Вход	<ul style="list-style-type: none"> <li>• Норма / На охране</li> <li>• Не норма / Снят с охраны</li> </ul>
Выход	<ul style="list-style-type: none"> <li>• Включен</li> <li>• Выключен</li> </ul>
Группа выходов	<ul style="list-style-type: none"> <li>• Включена</li> <li>• Выключена</li> </ul>
Временной блок	<ul style="list-style-type: none"> <li>• Активен</li> <li>• Не активен</li> </ul>



Логическая формула	<ul style="list-style-type: none"> <li>• Активна</li> <li>• Не активна</li> </ul>
--------------------	---

Основные

Описание:  Номер:

AND

AND

Описание

Признак входа	Кнопка выхода 2 (1.1_12)
Признак выход	Аварийное открывание (1.1_13)
Человек в шлюзе	Вход 1.1_14
_0_Усл. блокировки внутр. сч-ля	Реле замка 1 (1.1_01)
_0_Усл. блокировки внеш. сч-ля	LF3 = Группа 1.1_07
Шлюз в состоянии прохода	LF4 = (Группа 1.1_07 OR Группа 1.1_03) OR CMK1 (1.1_09)
Усл. блокировки внутр. сч-ля	LF5 = (Группа 1.1_07 OR Группа 1.1_04) OR CMK2 (1.1_11)
Усл. блокировки внеш. сч-ля	LF6 = Усл. блокировки внутр. сч-ля OR Усл. блокировки внеш. сч-ля
Разреш. откр. внеш. двери	LF7 = _0_Усл. блокировки внутр. сч-ля AND NOT Группа 1.1_11
Разреш. откр. внутр. двери	LF8 = _0_Усл. блокировки внеш. сч-ля AND NOT Группа 1.1_11
В шлюзе никого	LF10 = (NOT Группа 1.1_02 AND NOT CMK2 (1.1_11)) OR Группа 1.1_11
Следует вкл. реле внеш. двери	LF11 = (NOT Группа 1.1_01 AND NOT CMK1 (1.1_09)) OR Группа 1.1_11
Следует вкл. реле внутр. двери	LF12 = NOT Группа 1.1_07
	LF14 = Разреш. откр. внеш. двери AND Группа 1.1_01
	LF15 = Разреш. откр. внутр. двери AND Группа 1.1_02

1 из 13 (<= 48)

Рисунок 116 - Окно редактирования логических формул

Логические формулы могут являться источниками событий, при этом возможно назначение реакций на события панели «Активность логической формулы», «Неактивность логической формулы» (рисунок 117), либо использоваться в качестве условия выполнения реакции.

Редактирование логических формул осуществляется аналогично редактированию взаимодействий. Элементами в верхней части окна задаются устройства, используемые в формуле, а также логические операции. Имя формулы формируется автоматически и может быть изменено. В списке логических формул, находящемся в нижней части окна, для каждой формулы представлено также её полное описание

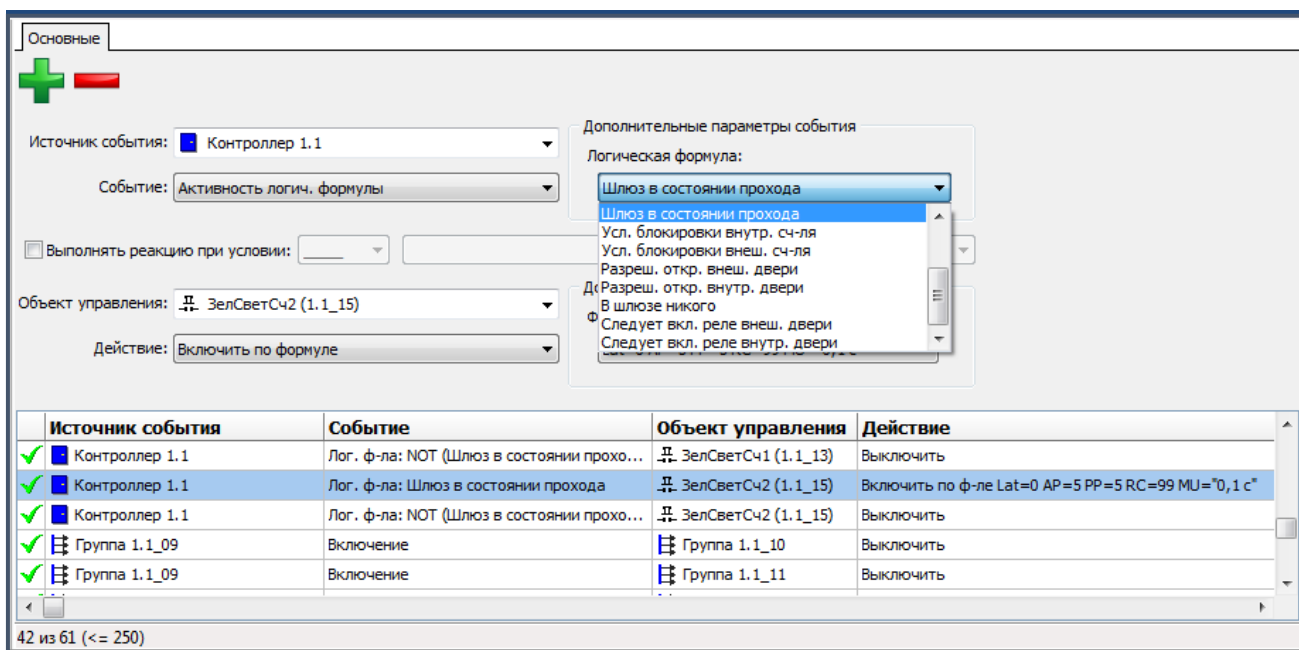


Рисунок 117 - Использование логических формул в качестве источника события

#### 9.1.4 Счётчики событий

Счётчики событий предназначены для подсчёта событий и выполнения реакций на изменение значения счётчика. Во взаимодействиях все события и команды, относящиеся к работе со счётчиками, отнесены к устройству «Панель».

На любое событие могут быть назначены реакции:

- увеличить значение счётчика;
- уменьшить значение счётчика;
- установить значение счётчика.

Аппаратные реакции могут быть назначены на события:

- равенство счётчика значению;
- равенство счётчика значению после увеличения значения;
- равенство счётчика значению после уменьшения значения.

Счётчики могут принимать значения от 0 до 63. Значение счётчика циклически изменяется, то есть при уменьшении значения счётчика, равного нулю, новое значение будет 63, и наоборот, при увеличении значения счётчика, равного 63, новое значение будет 0.

На рисунке 118 приведён практический пример использования счётчиков событий. Для помещения, оборудованного двусторонней дверью, реализовано ограничение доступа (т. е. запрещён доступ всем, кроме имеющих привилегию прохода при ограничении доступа) при количестве людей в помещении более четырёх. Для подсчёта количества людей

используются события «Штатный вход» и «Штатный выход». В полночь («Начало временного блока 3» и по включению питания счётчик обнуляется).

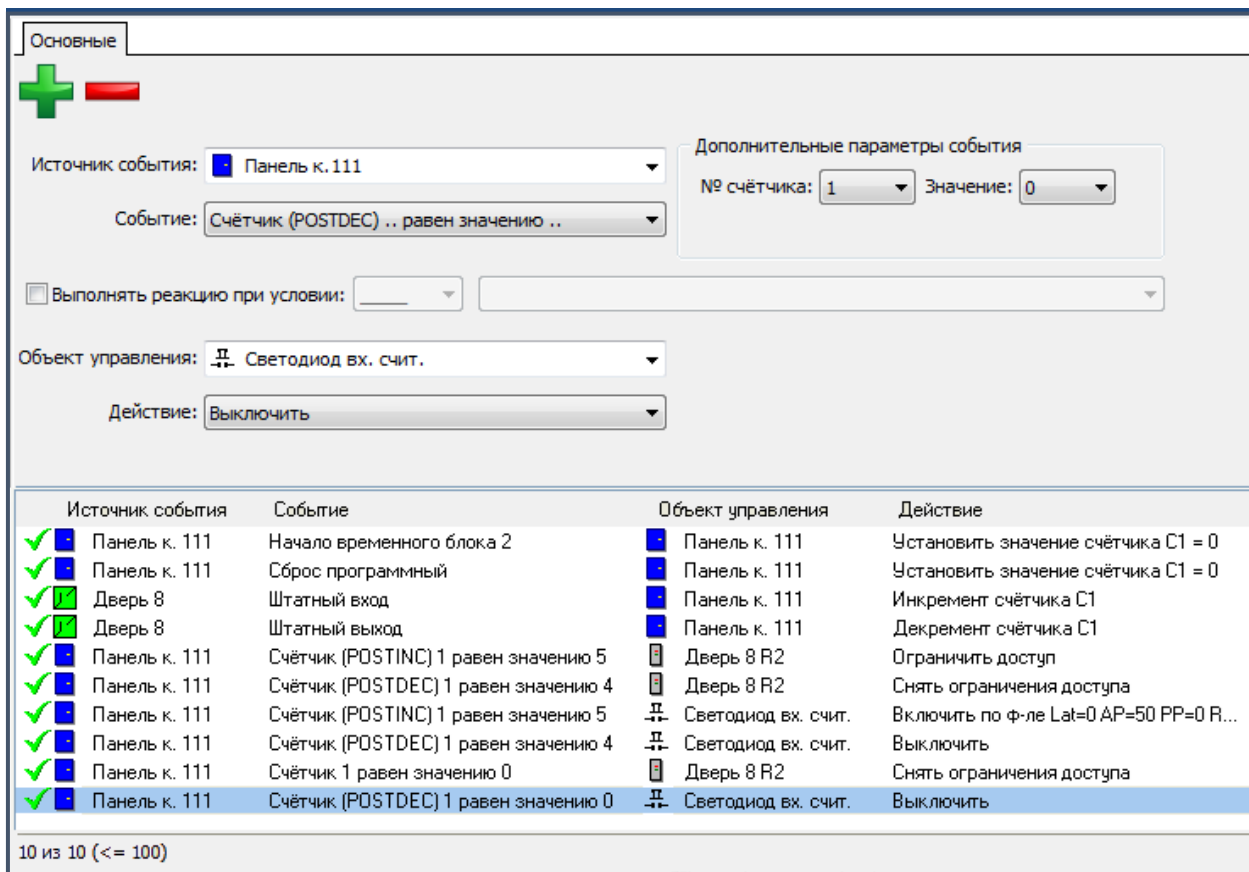


Рисунок 118 - Пример использования счётчиков событий

### 9.1.5 Взаимодействия между контроллерами

В СКУД Elsys существует возможность настройки взаимодействий между контроллерами, а также назначения реакций на потерю и восстановление связи с отдельными контроллерами.

Суть механизма, реализующего взаимодействия между контроллерами, в следующем. На любое событие может быть назначена реакция **«Панель->Сформировать сообщение контроллерам»** (рисунок 119). Номер событий может быть задан в диапазоне 1 – 64, причём в качестве адресата могут быть выбраны либо все контроллеры, либо один из них. В свою очередь, на любое событие с заданным номером (**«Панель->Сообщение от контроллера»**) от любого контроллера (или от конкретного) могут быть назначены реакции (рисунок 120).

**Внимание!** При отправке сообщения всем контроллерам, контроллер, от которого исходит сообщение отправляемое сообщение не получит.

Кроме того, существует возможность назначения реакций на потерю связи:

- с выбранным контроллером;

- с любым из контроллеров (взаимодействия обрабатываются, если до этого была связь со всеми контроллерами);
- с компьютером;

а также на восстановление связи:

- с выбранным контроллером;
- со всеми контроллерами;
- с компьютером.

Взаимодействия между контроллерами функционируют в пределах одной линии связи.

Кроме того, можно организовать взаимодействия между линиями связи (КСК или сетевой группы) под управлением сетевого контроллера, при этом, должна быть включена опция управляющего КСК «Транслировать межконтроллерные взаимодействия» (рисунок 23).

Организовать взаимодействия между контроллерами, подключенными к разным COM-портам нельзя.

**Внимание!** Для работы взаимодействий между контроллерами Elsys-MB в линии связи COM-порта и сетевого контроллера должен быть включен протокол MULTIMASTER. Для работы взаимодействий между контроллерами Elsys-MB-IP должен быть включен обмен сообщениями внутри сетевой группы.

Практический пример использования взаимодействий между контроллерами – реализация аварийной разблокировки точек эвакуации при пожарной тревоге и возвращения их в нормальный режим по окончании тревоги – приведён на рисунках 119 - 121.

Основные

Источник события: Вход подключения реле пожарной тревоги

Событие: Тревога

Выполнять реакцию при условии:

Объект управления: Контроллер 2.1 (Пожарная зона)

Действие: Сформировать сообщение контроллерам

Дополнительные параметры действия

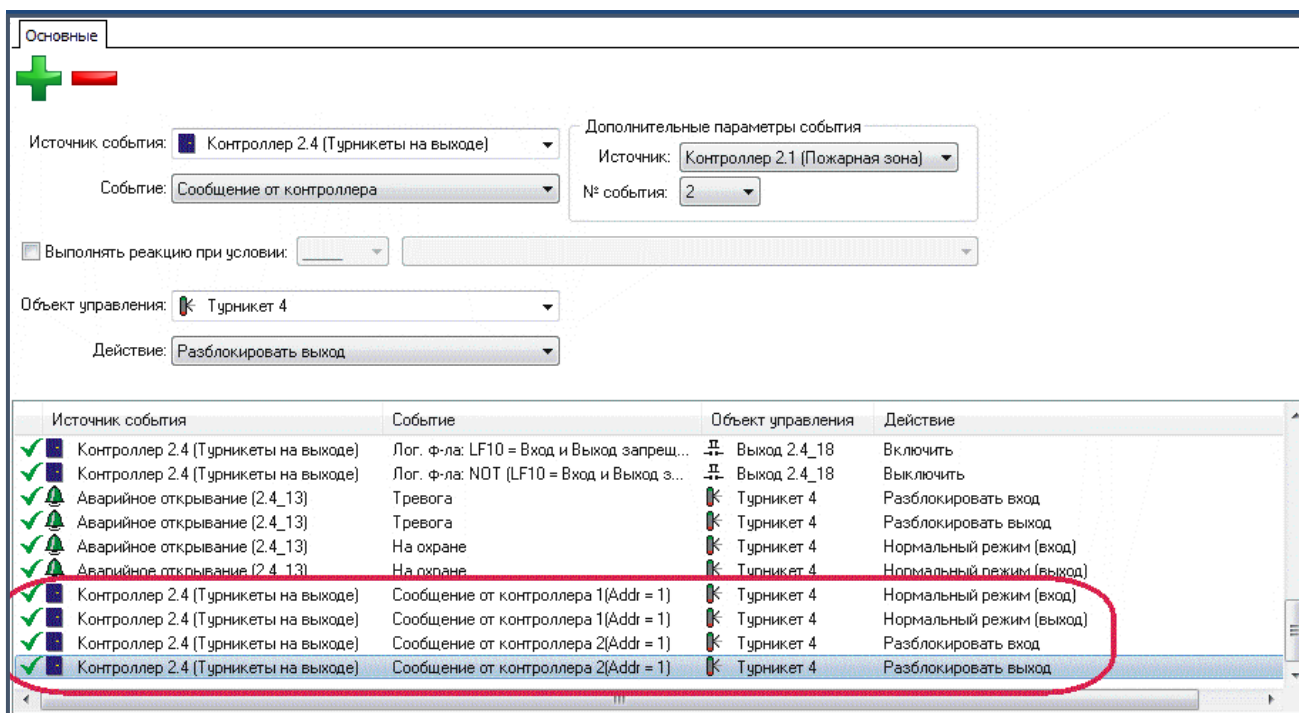
№ события: 2

Кому: Все контроллеры / Любой контро

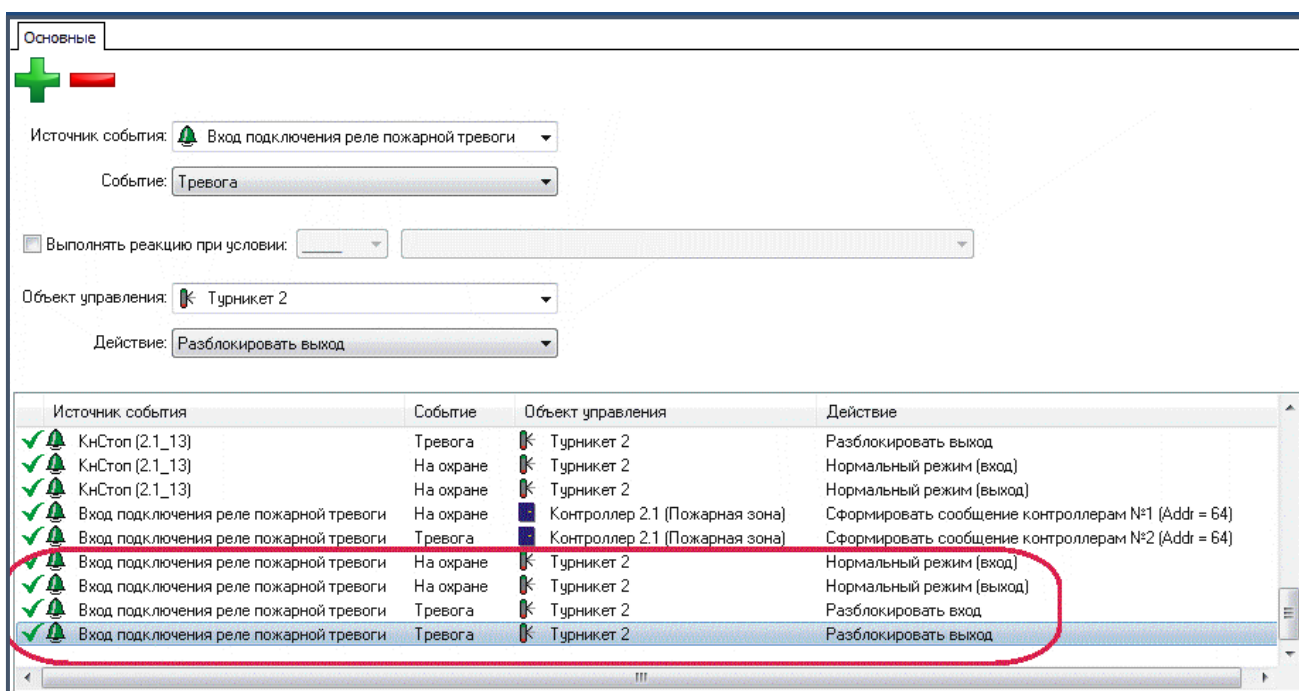
Источник события	Событие	Объект управления	Действие
Контроллер 2.1 (Пожарная зона)	Лог. фла: ...	КрСветСч2 (2.1_17)	Выключить
Контроллер 2.1 (Пожарная зона)	Лог. фла: ...	Выход 2.1_18	Включить
Контроллер 2.1 (Пожарная зона)	Лог. фла: ...	Выход 2.1_18	Выключить
КнСтоп (2.1_13)	Тревога	Турникет 2	Разблокировать вход
КнСтоп (2.1_13)	Тревога	Турникет 2	Разблокировать выход
КнСтоп (2.1_13)	На охране	Турникет 2	Нормальный режим (вход)
КнСтоп (2.1_13)	На охране	Турникет 2	Нормальный режим (выход)
Вход подключения реле пожарной тревоги	На охране	Контроллер 2.1 (Пожарная зона)	Сформировать сообщение контроллерам №1 (Addr = 64)
Вход подключения реле пожарной тревоги	Тревога	Контроллер 2.1 (Пожарная зона)	Сформировать сообщение контроллерам №2 (Addr = 64)

32 из 32 (<= 250)

**Рисунок 119 - Формирование сообщений №1-2 всем контроллерам от контроллера «Контроллер 2.1 (Пожарная зона)» при возникновении событий «Тревога» и «На охране» от входа подключения пожарной тревоги**



**Рисунок 120 – Реакции в контроллере «Контроллер 2.4 (Турникеты на выходе)» на сообщения №1-2 от контроллера «Контроллер 2.1 (Пожарная зона)»**



**Рисунок 121 – Реакции в контроллере «Контроллер 2.1 «Пожарная зона» на события «Тревога» и «На охране» от входа подключения реле пожарной тревоги**

При возникновении события «Тревога» от входа «Вход подключения реле пожарной тревоги» контроллера «Контроллер 2.1 (Пожарная зона)» всем контроллерам отправляется сообщение с номером 2, при возникновении события «На охране» - всем контроллерам отправляется сообщение с номером 1 (рисунок 119).

При получении сообщения 2 в контроллере «Контроллер 2.4 (Турникеты на выходе)» выполняется разблокировка точки прохода «Турникет 4», при приеме события 1 – точка турникет возвращается в нормальный режим (рисунок 120).

Следует отметить, что сообщения с номерами 1 и 2 отправляются всем контроллерам, кроме контроллера-источника сообщения «Контроллер 2.1 (Пожарная зона)». Чтобы выполнить аварийную разблокировку и возврат в нормальное состояние турникета «Турникет 2», подключенного к контроллеру «Контроллер 2.1 (Пожарная зона)», необходимо в этом контроллере назначить реакции непосредственно на события «Тревога» и «На охране» (рисунок 121).

### 9.1.6 Служебные PIN-коды

В контроллерах Elsys-MB имеется возможность назначения реакций на ввод отдельных PIN-кодов, а также на совместное предъявление PIN-кода и карты доступа. В каждом контроллере может быть запрограммировано до 16 служебных PIN-кодов (паролей), причём **ни один из этих кодов не должен совпадать ни с одним пользовательским PIN-кодом, и все пароли должны быть уникальными.**

Для редактирования списка PIN-кодов следует выбрать узел **«Служебные PIN-коды»** узла **«Взаимодействия»**, после чего в правой части экрана появится окно, изображённое на рисунке 122.

	№	PIN-код
✓	1	1234
✓	2	4321
✓	3	3333

Рисунок 122 - Редактирование служебных PIN-кодов

Добавление и редактирование PIN-кода осуществляется аналогично редактированию взаимодействий и формул.

В дальнейшем при настройке взаимодействий в качестве источников событий могут быть выбраны перечисленные ниже события, относящиеся к точкам доступа:

- ввод пароля на входном считывателе;

- ввод пароля на выходном считывателе;
- ввод пароля и предъявление карты на входном считывателе;
- ввод пароля и предъявление карты на выходном считывателе.

Все перечисленные события имеют параметр - номер PIN-кода. Кроме того, последние два события регистрируются в протоколе событий, причём каждое из них имеет 16 вариантов вида «Ввод PIN1 + PROX (вх. сч.)», «Ввод PIN2 + PROX (вх. сч.)», «Ввод PIN16 + PROX (вх. сч.)», каждый из которых представляет для ядра ПО «Бастион-2» отдельное событие.

Для пользователей, которым разрешено пользоваться служебными PIN-кодами, должна быть включена опция «Право ставить на охрану», в противном случае события типа «Ввод PINXX + PROX (...)» формироваться не будут.

При дальнейшей настройке ПО «Бастион-2» указанные события рекомендуется переименовать в соответствии с их смысловым значением (окно с настройками событий вызывается с помощью кнопки **«События»** на вкладке «Конфигурация», подробно – см. «Руководство администратора «Бастион-2»»). На рисунке 123 приведен практический пример использования служебных PIN-кодов для авторизованного управления режимами охраны.

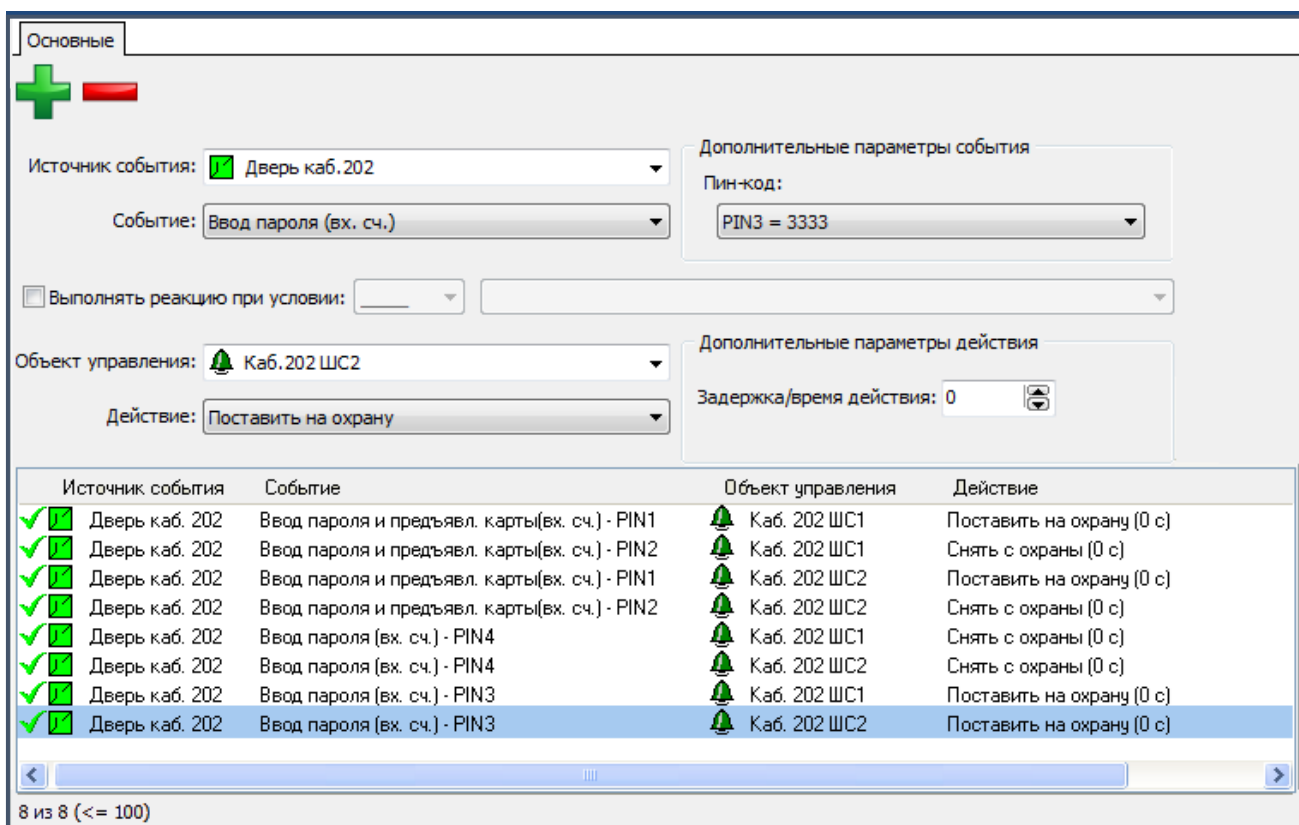


Рисунок 123 - Назначение реакций на ввод служебных PIN-кодов

На рисунке 124 изображён вид событий авторизованного управления в окне штатных сообщений ПО «Бастион-2» до (первые 6 событий) и после (следующие 6 событий) переименования.



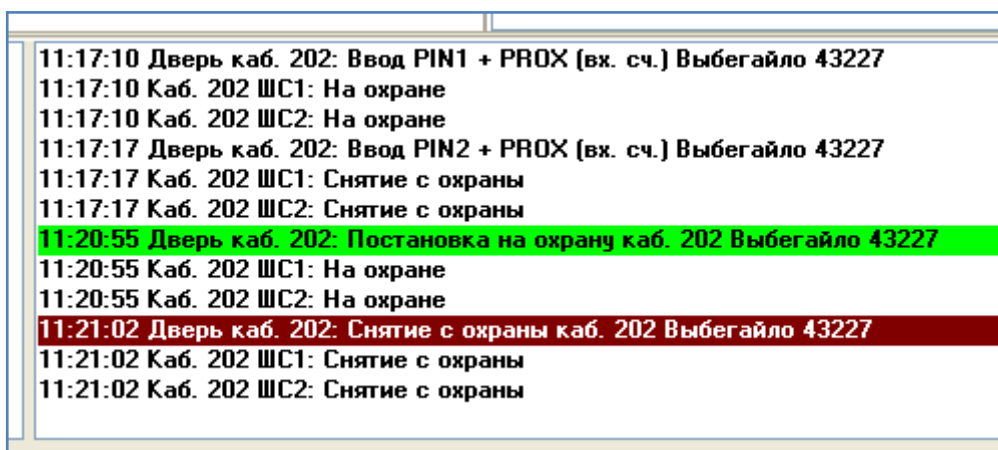


Рисунок 124 - Вид событий авторизованного управления в окне штатных сообщений

### 9.1.7 Назначение реакций на предъявление отдельных карт доступа

В контроллерах Elsys-MB могут быть назначены реакции на предъявление отдельных карт доступа (рисунок 125). В качестве служебной карты может быть назначен любой из выданных пропусков. Всего во взаимодействиях в каждом контроллере могут участвовать не более 48 служебных карт.

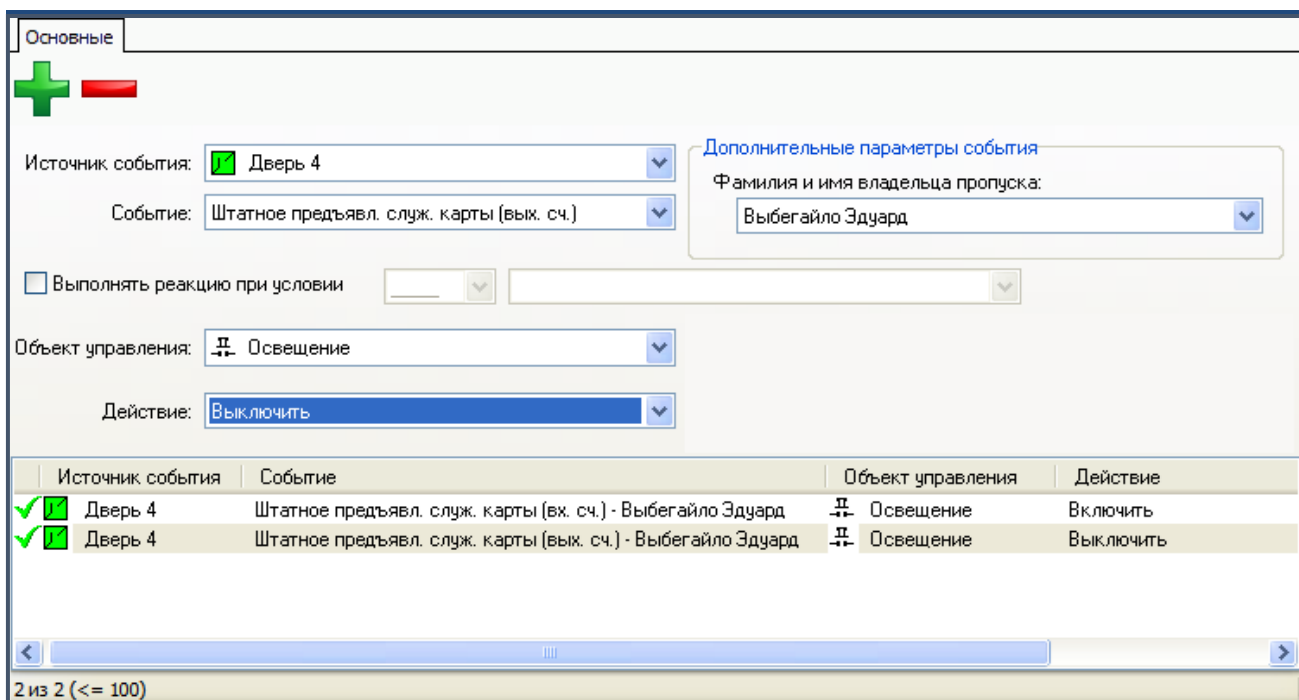


Рисунок 125 - Назначение реакций на предъявление отдельных карт доступа

Назначение реакций возможно на перечисленные ниже события точек доступа:

- штатное предъявление служебной карты входному считывателю;
- штатное предъявление служебной карты выходному считывателю;
- предъявление служебной карты входному считывателю;
- предъявление служебной карты выходному считывателю.



Первые два события обрабатываются, если полномочия разрешают доступ (с учётом анализа уровня доступа, временной зоны и зоны доступа), а последние два – при любом предъявлении карты.

На рисунке 125 приведён простейший пример использования описанной возможности – при входе в помещение включается освещение на конкретном рабочем месте. При использовании взаимодействий между контроллерами легко реализуются и более сложные функции. Например, сотрудник предъявляет карту на проходной предприятия, и по этому событию в его кабинете заранее включается кондиционер.

### 9.1.8 Назначение реакций на удержание ключа/карты

В контроллерах Elsys-MB версий 2.60 и выше предусмотрена возможность контроля нахождения карты доступа в зоне действия считывателя. Эта возможность может быть реализована только при подключении считывателей по интерфейсу Touch Memory, так как только в этом режиме считыватель передаёт код карты непрерывно, пока она находится в зоне действия считывателя.

Для использования режима контроля удержания карты необходимо выполнение следующих условий:

- считыватель должен быть подключен по интерфейсу Touch Memory;
- в свойствах контроллера настройка «Интерфейс считывателей» должна иметь значение «Touch Memory»;
- в свойствах выбранного считывателя должна быть включена настройка «Анализировать удержание ключа/карты»;
- в дополнительных опциях пропуска, задаваемых профилем настроек персонала (рисунок 126), должна быть включена опция «Право ставить на охрану».

Если используется этот режим, кратковременное предъявление карты будет формировать событие «Предоставление доступа» (формируется в момент отпускания карты/ключа), а удержание свыше заданного времени будет интерпретироваться как удержание карты. Время, в течение которого необходимо удерживать карту или ключ для формирования события «Удержание карты/ключа», задаётся в настройках считывателя (вкладка «Дополнительные», опция «Интервал при постановке на охрану» на рисунке 76) и имеет диапазон значений от 1 до 120 с (по умолчанию – 3 с).

Если у выбранного считывателя назначен раздел для управления и индикации, удержание карты/ключа будет вызывать действие по управлению режимом охраны раздела (постановку на охрану или снятие с охраны). Если раздел для управления и индикации не назначен, при удержании карты или ключа будет сформировано событие «Удержание карты/ключа» (регистрируется в протоколе и может участвовать во взаимодействиях), а по окончании удержания – событие «Отпускание карты/ключа» (может участвовать во взаимодействиях, но не регистрируется в протоколе).

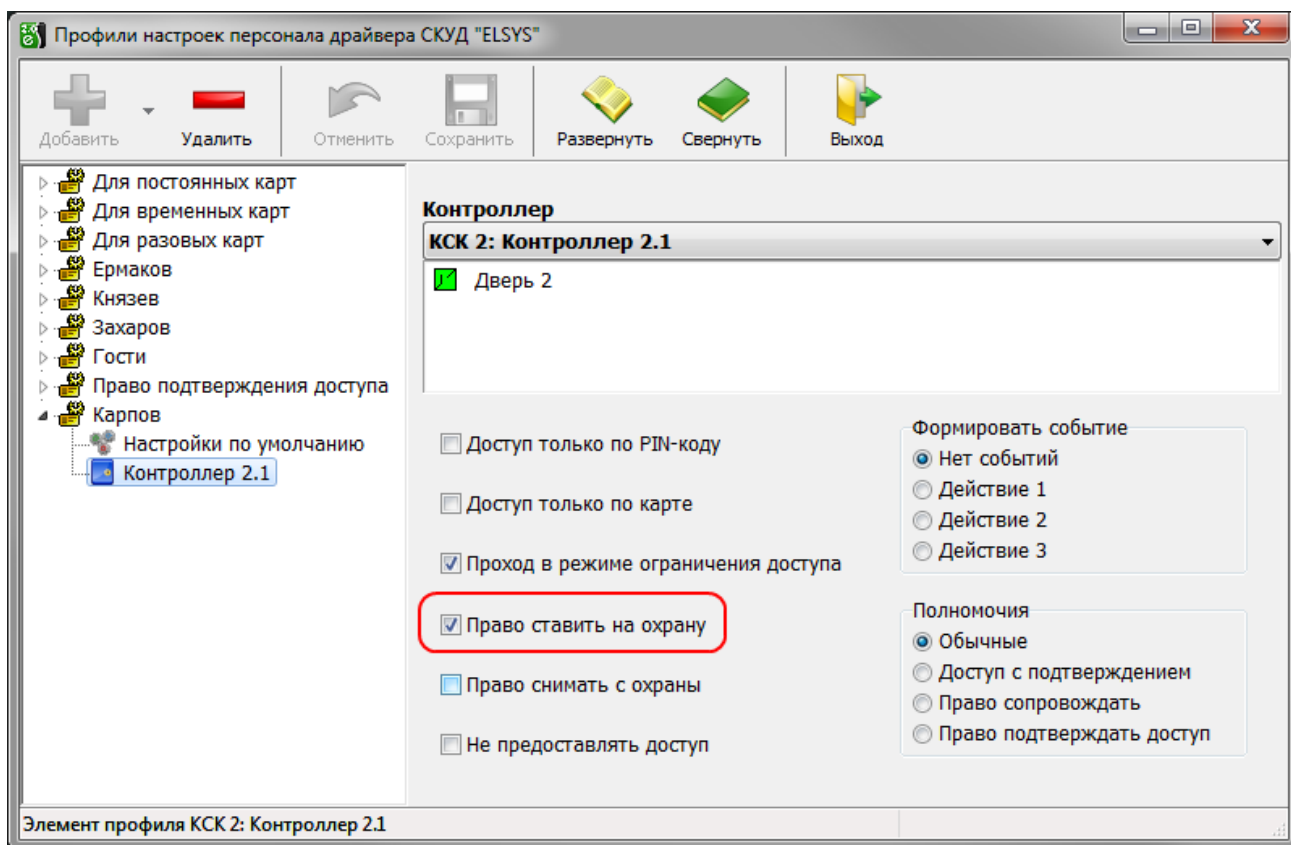


Рисунок 126 – Профили настроек персонала

Одно из возможных применений использования описываемой возможности – ручное ограничение режима доступа в помещение (например, если в кабинете руководителя проходит совещание). Для реализации этой функции необходимо настроить взаимодействия, как показано на рисунке 127.

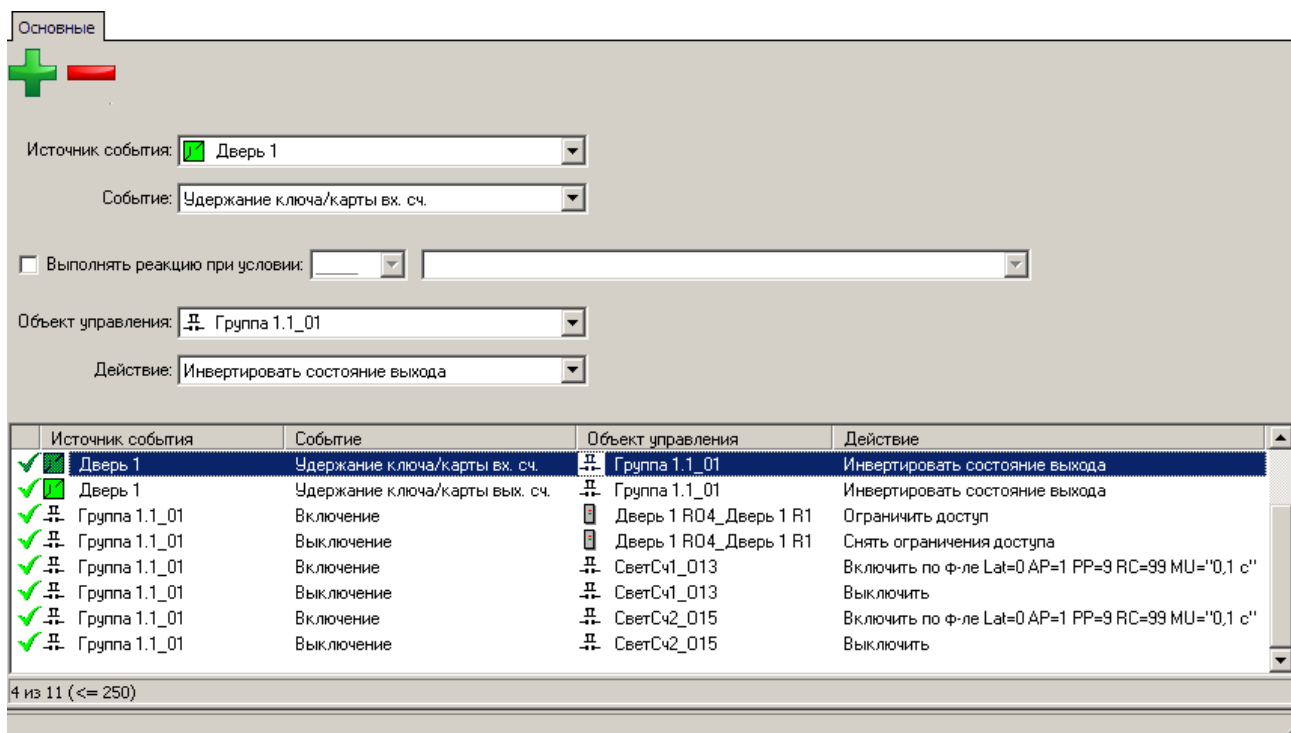


Рисунок 127 – Настройка взаимодействий для реализации режима ограничения доступа

В конфигурацию контроллера добавляется вспомогательное устройство – группа выходов «Группа 1.1.\_01» (выходы включать в её состав не нужно). Каждое событие «Удержание карты» переключает состояние вспомогательной группы выходов. Если группа переходит в состояние «Включено», включается режим ограничения доступа, а светодиоды считывателей переходят в мигающий режим (0,9 с горит красный, 0,1 с - зелёный). При переходе группы в состояние «Выключено», считыватели переходят в обычный режим работы.

Для сотрудников, которые должны всегда иметь право доступа в помещение, следует включить опцию «Проход в режиме ограничения доступа».

Ещё один пример применения контроля удержания карты – включение заданного выхода на время удержания карты (рисунок 128). Эта функция может использоваться, например, для управления освещением в гостиничных номерах.

✓	Дверь 3	Удержание ключа/карты вх. сч.	⚙	Выход 2.6_03	Включить
✓	Дверь 3	Отпускание ключа/карты вх. сч.	⚙	Выход 2.6_03	Выключить
✓	Дверь 4	Удержание ключа/карты вх. сч.	⚙	Выход 2.6_04	Включить
✓	Дверь 4	Отпускание ключа/карты вх. сч.	⚙	Выход 2.6_04	Выключить

Рисунок 128 – Настройка взаимодействий для включения выходов на время удержания карты

Кроме того, событие «Удержание ключа/карты» может использоваться для назначения реакций в ПО «Бастион-2», обеспечивая интеграцию с другими подсистемами.

## 9.1.9 Настройка управления по временным расписаниям

### 9.1.9.1 Настройка временных расписаний

Временные расписания используются для разграничения полномочий пользователей по времени, а также для управления объектами (включение исполнительных устройств, изменение режимов точек доступа и т. п.).

Настройка временных расписаний производится в бюро пропусков.

Чтобы вызвать окно с настройками временных расписаний следует в главном окне бюро пропусков перейти на вкладку «Основное» и на ленте «Словари» нажать кнопку «Временные зоны...» (рисунок 129).

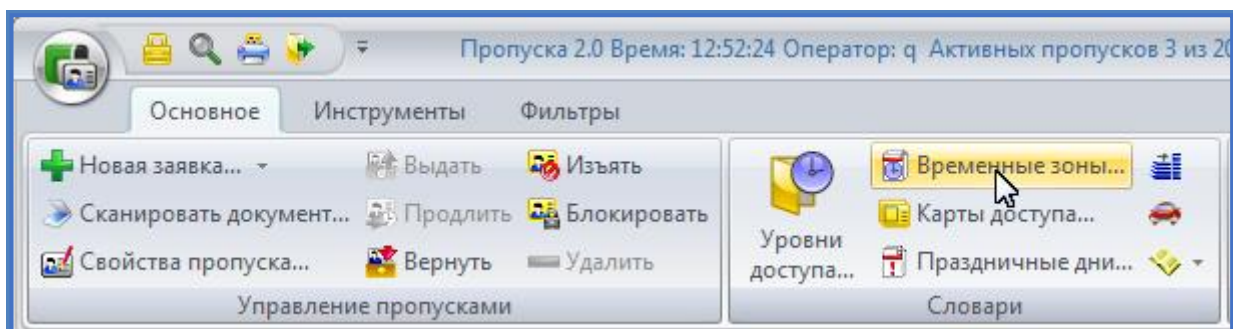


Рисунок 129 – Вызов окна для настройки временных блоков

Временное расписание представляет собой временной блок (рисунок 130), который включает один или несколько временных интервалов (временных зон) (рисунок 131).

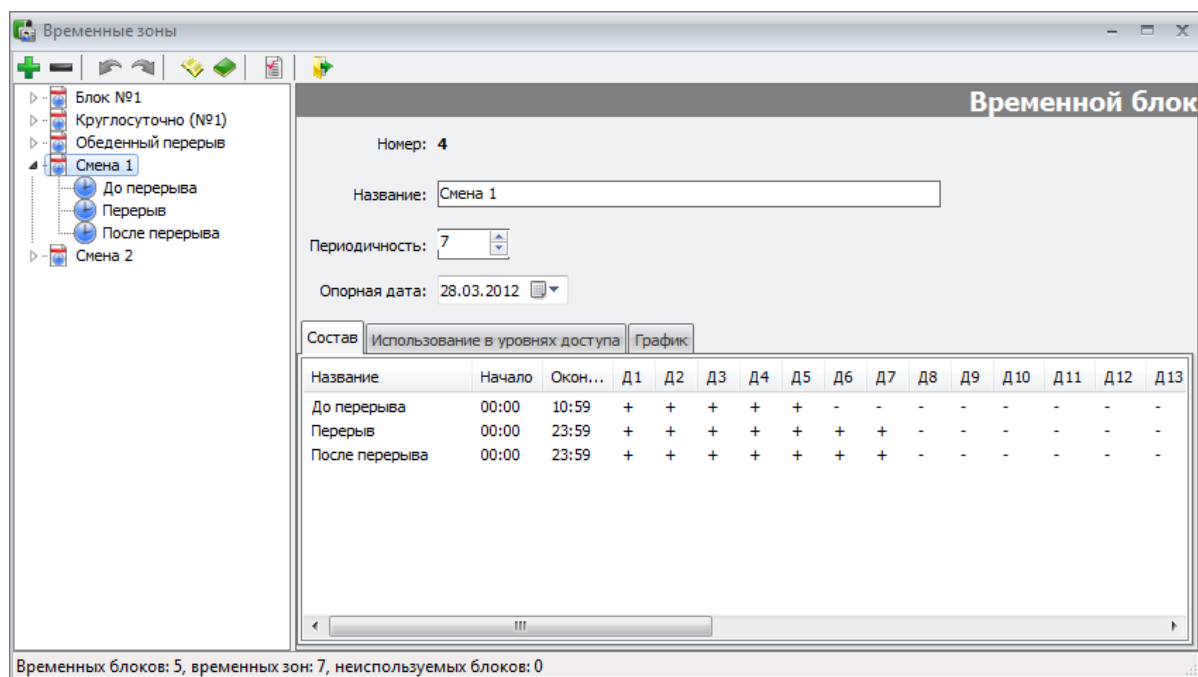


Рисунок 130 - Состав временного блока

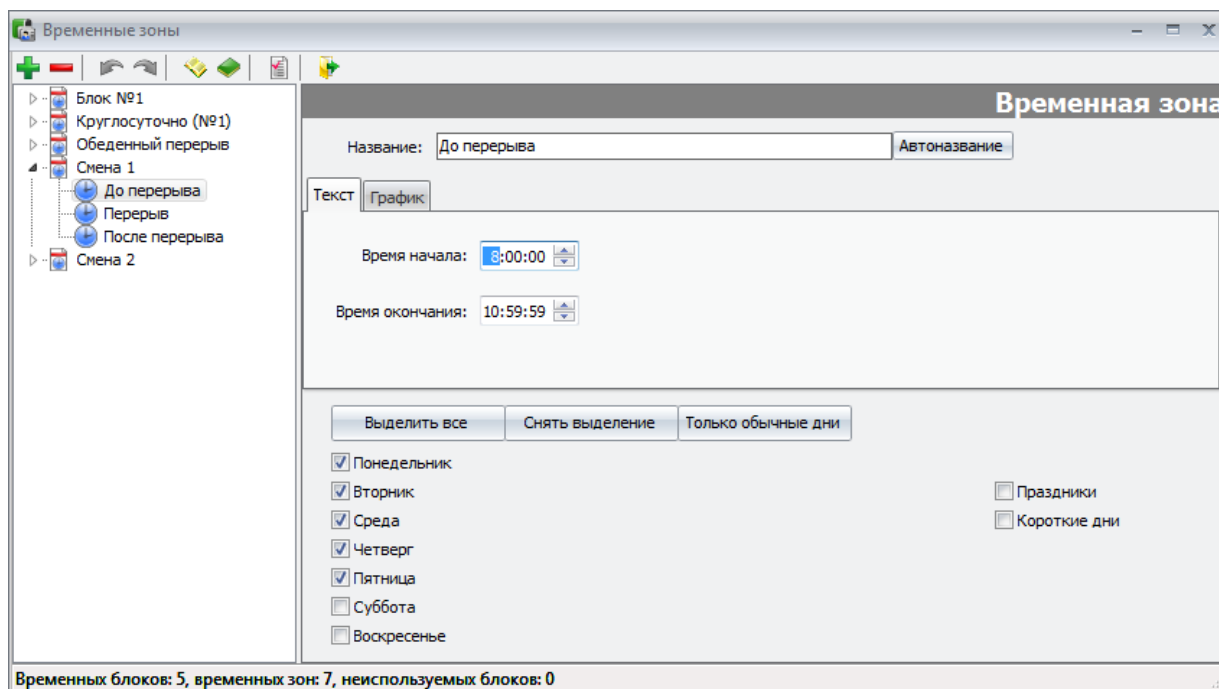


Рисунок 131 – Настройка параметров временных интервалов (временных зон)

Временной интервал описывается следующими параметрами (рисунок 131):

- номер временного блока, к которому он относится;
- начало временного интервала (часы, минуты);
- окончание временного интервала (часы, минуты);
- периодичность графика (от 2 до 31, значение 7 соответствует недельному графику);

- дата начала работы графика (для скользящих графиков одновременно является опорной датой, относительно которой отсчитываются дни графика; для недельного графика играет роль, если задана дата окончания работы графика);
- дата окончания работы графика (если не задана или равна дате начала работы графика, это ограничение при анализе временного расписания не проверяется);
- активные дни графика (дни недели – для недельных графиков, дни с номерами 1..31 – для скользящих графиков; праздничные дни двух типов);
- опция «Не использовать праздничные дни».

В составе уровня доступа различные временные блоки могут быть назначены для разных считывателей.

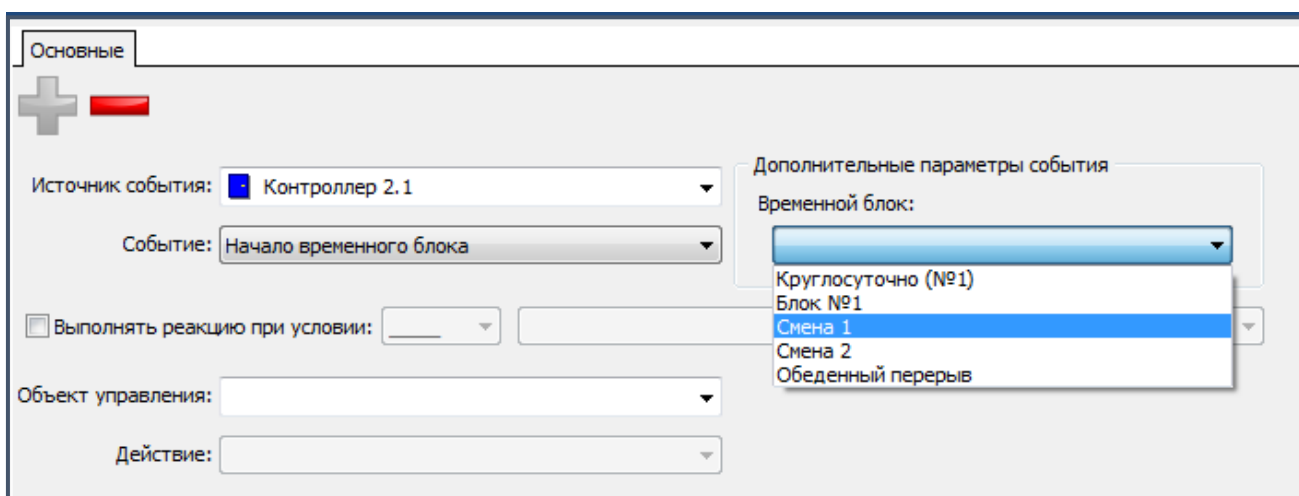
Настройка временных расписаний (временных блоков) подробно описана в руководстве оператора/администратора бюро пропусков.

#### 9.1.9.2 Настройка взаимодействий по временным расписаниям

Для настройки взаимодействий по временным расписаниям следует на странице свойств «Взаимодействия» для требуемого контроллера добавить новое взаимодействие и в качестве источника события выбрать контроллер.

Настройку «Событие» установить в значение «Начало временного блока» или «Окончание временного блока», в зависимости от требуемого управления (рисунок 132) и указать требуемый временной блок.

**Внимание!** В ПО «Бастион-2» при настройке взаимодействий номер временного блока должен быть в диапазоне 1..125.



The screenshot shows a configuration window titled 'Основные' (Basic). It contains several fields for setting up an interaction:

- Источник события:** (Event Source) dropdown menu with 'Контроллер 2.1' (Controller 2.1) selected.
- Событие:** (Event) dropdown menu with 'Начало временного блока' (Start of time block) selected.
- Дополнительные параметры события:** (Additional event parameters) section with a dropdown menu for 'Временной блок:' (Time block:). The menu is open, showing options: 'Круглосуточно (№1)' (Round-the-clock (№1)), 'Блок №1' (Block №1), 'Смена 1' (Shift 1), 'Смена 2' (Shift 2), and 'Обеденный перерыв' (Lunch break). 'Смена 1' is highlighted.
- Выполнять реакцию при условии:** (Perform reaction when condition) checkbox and dropdown menu.
- Объект управления:** (Control object) dropdown menu.
- Действие:** (Action) dropdown menu.

Рисунок 132 – Настройка взаимодействий по временным расписаниям

Далее, как и при настройке других взаимодействий следует выбрать объект управления и назначить команду управления.

Примеры настройки управления по временным расписаниям приведены на рисунке (рисунок 133).

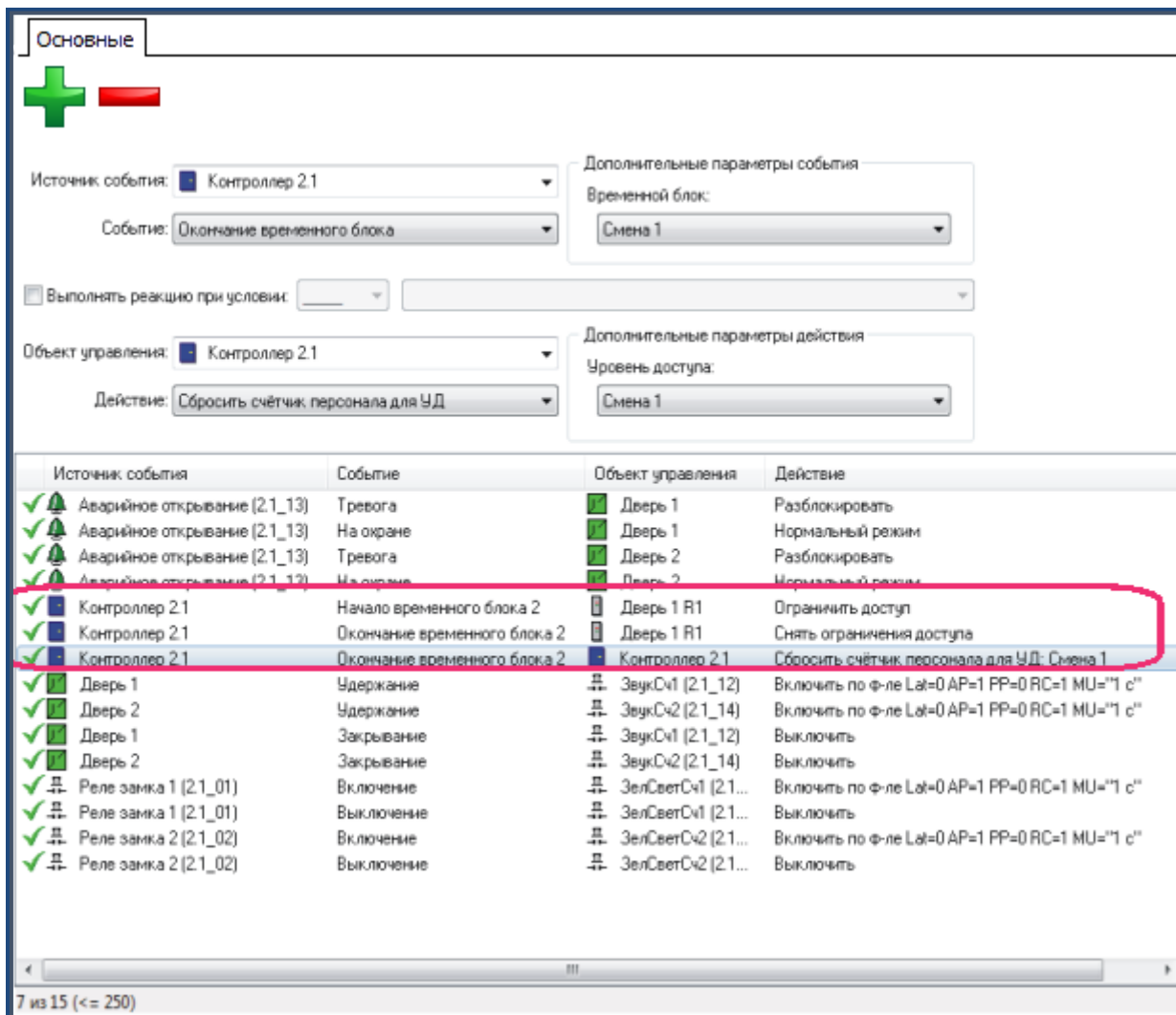


Рисунок 133 – Настройка управления по временным расписаниям

### 9.1.9.3 Настройка логических формул с использованием временных расписаний

При составлении логических формул в логических условиях могут использоваться временные блоки. При этом могут быть использованы условие активности временного блока (состояние «Активен») или условие неактивности временного блока (состояние «Не активен»).

Временной блок считается активным, если хотя бы один временной интервал, входящий в его состав, активен. Временной интервал считается активным, если текущее время находится внутри границ временного интервала и если текущий день разрешён в этом временном интервале.

Пример использования временных блоков при составлении логических формул показан на рисунке 134.

Основные

Описание:  Номер:

(

OR

AND

Описание	Подробное описание формулы
✓ LF1 = Разрешение ОткрВыход	LF1 = (NOT Группа 2.1_01 AND NOT КнЗакреть (2.1_12)) AND LF8 = ВходРазрешён
✓ LF2 = Разрешение ОткрВход	LF2 = NOT Вход 2.1_14 AND NOT КнЗакреть (2.1_12)
✓ LF3 = РазрешНормРеж	LF3 = NOT КнОткрыть(2.1_11) AND NOT Вход 2.1_14
✓ LF4 = УсловиеПолнойРазблокировки	LF4 = (КнОткрыть(2.1_11) AND КнЗакреть (2.1_12)) AND Вход 2.1_14
✓ LF5 = УслРазблокВх	LF5 = (КнОткрыть(2.1_11) AND КнЗакреть (2.1_12)) AND NOT Вход 2.1_14
✓ LF6 = УслРазблокВых	LF6 = (NOT КнОткрыть(2.1_11) AND КнЗакреть (2.1_12)) AND Вход 2.1_14
✓ LF7 = ВклНормРежПриОтпусканииСтоп	LF7 = (NOT КнОткрыть(2.1_11) AND NOT Вход 2.1_14) AND Группа 2.1_01
✓ LF8 = ВходРазрешён	LF8 = ЗелСветСч1 (2.1_13)
✓ LF9 = ВыходРазрешён	LF9 = ЗелСветСч2 (2.1_15)
✓ LF10 = Вход и Выход запрещены	LF10 = NOT ЗелСветСч1 (2.1_13) AND NOT ЗелСветСч2 (2.1_15)
✓ Работа первой смены	LF11 = Смена 1
✓ Работа второй смены	LF12 = Смена 2
✓ Обеденный перерыв	LF13 = Обеденный перерыв
✓ Первая смена и обеденный перерыв	LF14 = Смена 1 OR Обеденный перерыв
✓ Вторая смена и обеденный перерыв	LF15 = Смена 2 OR Обеденный перерыв

Рисунок 134 - Использование временных блоков в логических формулах

### 9.1.10 Настройка функций, связанных с подсчётом персонала

В контроллерах Elsys-MB предусмотрена возможность ведения подсчёта персонала в областях контроля (зонах доступа), обслуживаемых каждым контроллером. Для работы этой функции необходимо выполнение следующих условий:

- наличие модуля расширения памяти;
- должна быть включена опция «Расширенные возможности настройки».

**Внимание!** Следует помнить, что описываемые в настоящей главе функции подсчёта персонала и автоматическая постановка на охрану при выходе последнего сотрудника (см. п. 9.3) работают и настраиваются независимо друг от друга.

Функция подсчёта персонала может быть включена для любой двусторонней точки доступа. Для использования этой функции необходимо включить опцию **«Вести подсчёт количества персонала в областях контроля»** (рисунок 63) .

Подсчёт персонала работает следующим образом. После каждого события «Штатный вход» или «Штатный выход» контроллер обновляет текущую зону доступа сотрудника. Затем, анализируя текущее месторасположение каждого сотрудника, контроллер пересчитывает и обновляет общее число сотрудников, находящихся во внутренней зоне



доступа. Подсчёт числа сотрудников, находящихся во внутренней зоне доступа, выполняется также для каждого из уровней доступа. Если включен глобальный контроль последовательности прохода, для подсчёта количества сотрудников используются также события от других контроллеров о перемещении пользователей.

При включенной функции подсчёта персонала формируются следующие события:

- «Штатный вход первого сотрудника»;
- «Штатный выход последнего сотрудника»;
- «Штатный вход первого сотрудника с заданным уровнем доступа»;
- «Штатный выход последнего сотрудника с заданным уровнем доступа».

Перечисленные события могут участвовать в аппаратных взаимодействиях. Если эти события необходимо регистрировать в протоколе и передавать в ПК (например, для интеграции с другими подсистемами), следует использовать опции **«Регистрировать вход первого и выход последнего»** и **«Регистрировать вход первого и выход последнего (для каждого уровня доступа)»**.

В контроллерах Elsys-MB предусмотрена возможность назначения счётчиков событий для подсчёта количества персонала. Для задания связи точки доступа со счётчиком событий необходимо использовать вспомогательные события «Изменение количества персонала» и «Изменение количества персонала с заданным уровнем доступа», на которые должны быть назначены команды «Установить значение счётчика» (рисунок 135).

Источники событий	События	Объекты управления
✓ [Тревога]	Тревога	✓ Дверь 1_PRO4
✓ [На охране]	На охране	✓ Дверь 1_PRO4
✓ [Сброс программный]	Сброс программный	PRO4Doors2
✓ [Изменение количества персонала с заданным УД: PRO4_ONLY]	Изменение количества персонала с заданным УД: PRO4_ONLY	PRO4Doors2
✓ [Счётчик (POSTINC) 1 равен значению 2]	Счётчик (POSTINC) 1 равен значению 2	Выход 2.1_03
✓ [Счётчик (POSTDEC) 1 равен значению 1]	Счётчик (POSTDEC) 1 равен значению 1	Выход 2.1_03
✓ [Изменение количества персонала с заданным УД: По умолчанию]	Изменение количества персонала с заданным УД: По умолчанию	PRO4Doors2
✓ [Счётчик (POSTINC) 2 равен значению 2]	Счётчик (POSTINC) 2 равен значению 2	Выход 2.1_04
✓ [Счётчик (POSTDEC) 2 равен значению 1]	Счётчик (POSTDEC) 2 равен значению 1	Выход 2.1_04
✓ [Взлом]	Взлом	Замок1_01 (PRO4Doors2)
✓ [Изменение количества персонала с заданным УД: По умолчанию]	Изменение количества персонала с заданным УД: По умолчанию	PRO4Doors2

Рисунок 135 – Настройка взаимодействий для подсчёта количества персонала



В отличие от других взаимодействий, это взаимодействие не выполняется, но обеспечивает автоматическую загрузку значения счётчика событий № 1 числовым значением количества персонала во внутренней зоне точки доступа. Устанавливаемое значение счётчика роли не играет. На события «Изменение количества персонала» и «Изменение количества персонала с заданным уровнем доступа» любые другие реакции назначены быть не могут – они выполняться не будут. Счётчик событий, назначенный таким образом для подсчёта персонала, может быть использован во взаимодействиях как источник событий (см. п. 9.1.4), что даёт дополнительные возможности для программирования логики работы. Например, при увеличении количества персонала свыше какого-то значения (например, более 5 человек в помещении), может быть включено ограничение доступа.

После инициализации счётчик персонала находится в неопределённом состоянии, так как текущее местоположение сотрудников неизвестно. Поэтому, для корректной работы подсчёта персонала обязательно должен выполняться сброс счётчика персонала – например, по факту постановки помещения на охрану, при выполнении сброса или по событию от других подсистем «Бастион-2». Для установки текущего местоположения сотрудников в состояние «Внешняя зона» (соответствует состоянию, при котором во внутренней зоне никого нет) предусмотрены команды, выполняемые через взаимодействия (источник события – контроллер) – «Сбросить счётчик персонала» и «Сбросить счётчик персонала для УД» (рисунок 136).

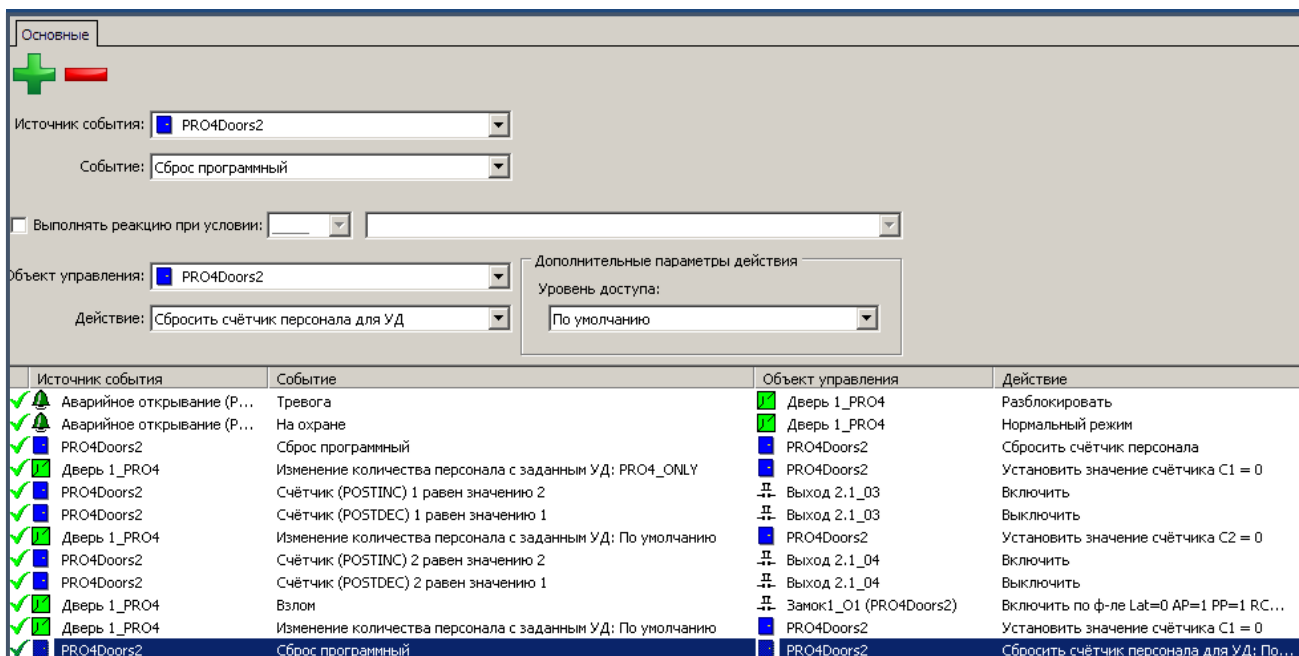


Рисунок 136 – Настройка взаимодействий для сброса счетчиков персонала

## 9.2 Профили настроек персонала

Помимо значений, идентифицирующих пропуск (номер и сайт-код карты, PIN-код) и определяющих его основные полномочия (номер уровня доступа), в СКУД Elsys для каждого пропуска могут быть заданы дополнительные полномочия - профили настроек персонала.

Профиль настроек персонала в драйвере Elsys представляет собой совокупность аппаратных настроек контроллеров, которые можно назначить одному и нескольким пропускам.

Для настройки профилей используется конфигуратор, который вызывается с помощью кнопки «**Профили настройки персонала**» на ленте управления драйвера Elsys (рисунок 137).

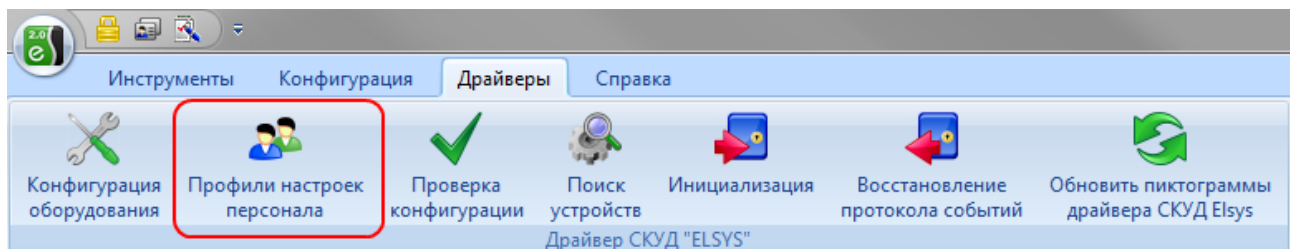


Рисунок 137 - Кнопка вызова конфигулятора профилей персонала

Пользовательский интерфейс конфигулятора профилей персонала аналогичен интерфейсу конфигулятора оборудования драйвера «Бастион-2 – Elsys» и других программных модулей ПО «Бастион-2» (рисунок 138).

Описание кнопок панели управления конфигулятора профилей приведено в таблице 18.

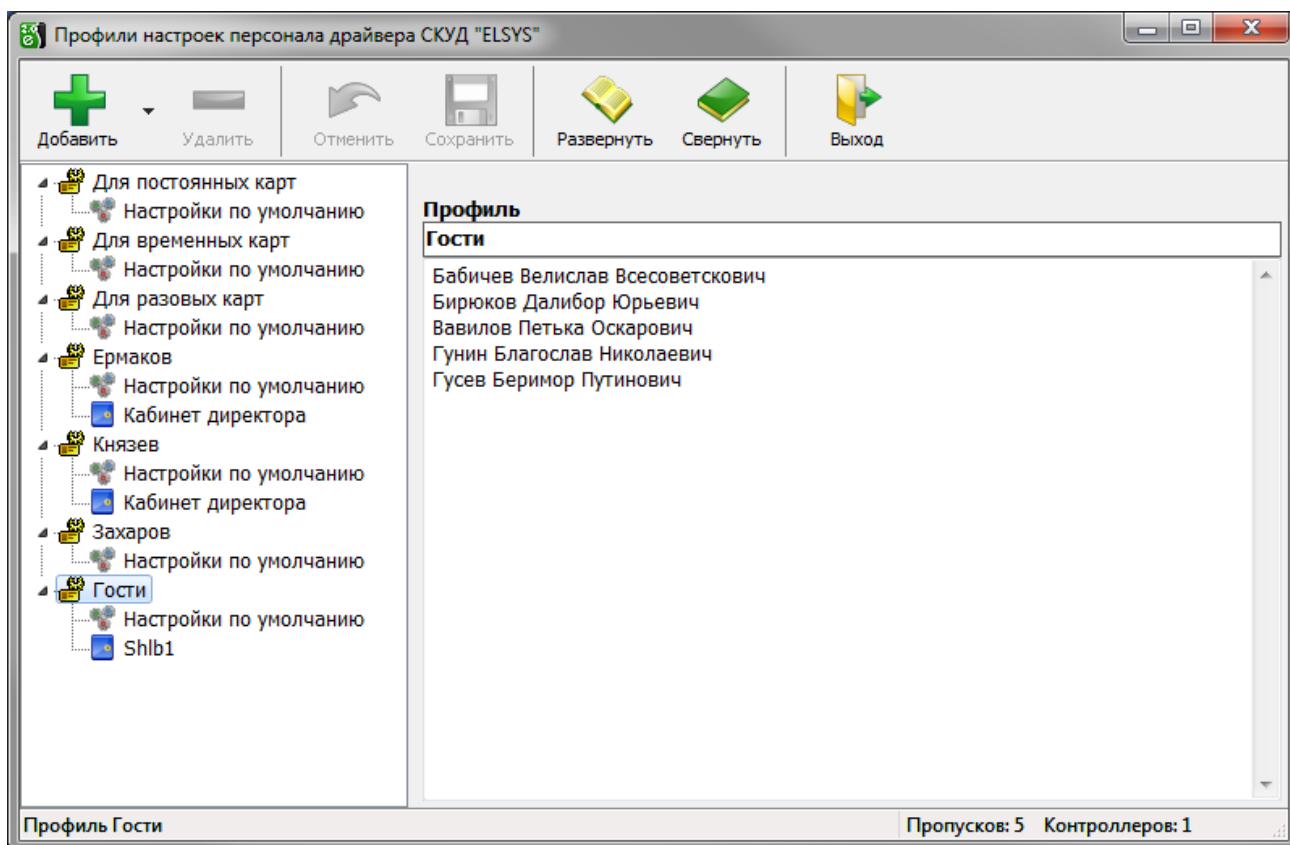


Рисунок 138 - Окно конфигулятора профилей персонала

Таблица 18 - Назначение кнопок панели управления конфигуратора профилей персонала

Кнопка	Наименование	Назначение
	«Добавить»	Добавляет новый профиль или элемент профиля в конфигурацию. Функция также доступна из контекстного меню дерева конфигурации.
	«Удалить»	Удаляет существующие профиль или элемент профиля из конфигурации. Функция также доступна из контекстного меню выбранного узла.  Функция недоступна для predetermined профилей, а также для профилей, которые используются хотя бы одним пропуском.
	«Отменить»	Отменить внесённые изменения.  Выполняется загрузка последней сохранённой конфигурации из базы данных.
	«Сохранить»	Сохранить внесённые изменения.  Выполняется сохранение конфигурации в базу данных.
	«Развернуть»	Разворачивает все узлы дерева конфигурации.
	«Свернуть»	Сворачивает все узлы дерева конфигурации.
	«Выход»	Выход из конфигуратора.

В левой части окна конфигуратора расположено дерево профилей настроек персонала, в котором имеется два типа узлов: узлы профилей и дочерние для них узлы (элементы профилей). В правой части окна расположена панель, предназначенная для настройки и просмотра свойств узла.

Изначально существует три predetermined профиля, которые назначаются по умолчанию пропускам в бюро пропусков в соответствии с их типом:

- Профиль «Для постоянных карт»;
- Профиль «Для временных карт»;
- Профиль «Для разовых карт».

Predetermined профили удалить нельзя, а их наименование недоступно для редактирования. Все остальные функции доступны как для обычных профилей, добавленных пользователем.

Конфигуратор профилей персонала позволяет создавать новые профили персонала, устанавливать настройки профилей по умолчанию, добавлять в профили дочерние элементы (контроллеры) и устанавливать для них собственные настройки.

Добавленный пользователем профиль может быть в дальнейшем назначен любому пропуску в бюро пропусков. В свойствах профиля (рисунок 138) отображается список персон, в пропусках которых назначен данный профиль. Добавленный пользователем профиль можно удалить, если он не назначен ни одному пропуску.

Настройки профиля по умолчанию (рисунок 139) и настройки элемента профиля - контроллера (рисунок 140), идентичны по составу. Их описание приводится ниже.

**«Доступ только по PIN-коду»** и **«Доступ только по карте»** - эти настройки определяют, какие устройства используются для идентификации пользователя. Если обе опции выключены и точка доступа оборудована считывателем и клавиатурой, для предоставления доступа необходимо набрать PIN-Код и предъявить карту. Если включена первая опция, то для получения доступа достаточно набрать PIN-код, а если включена вторая – достаточно предъявить карту.

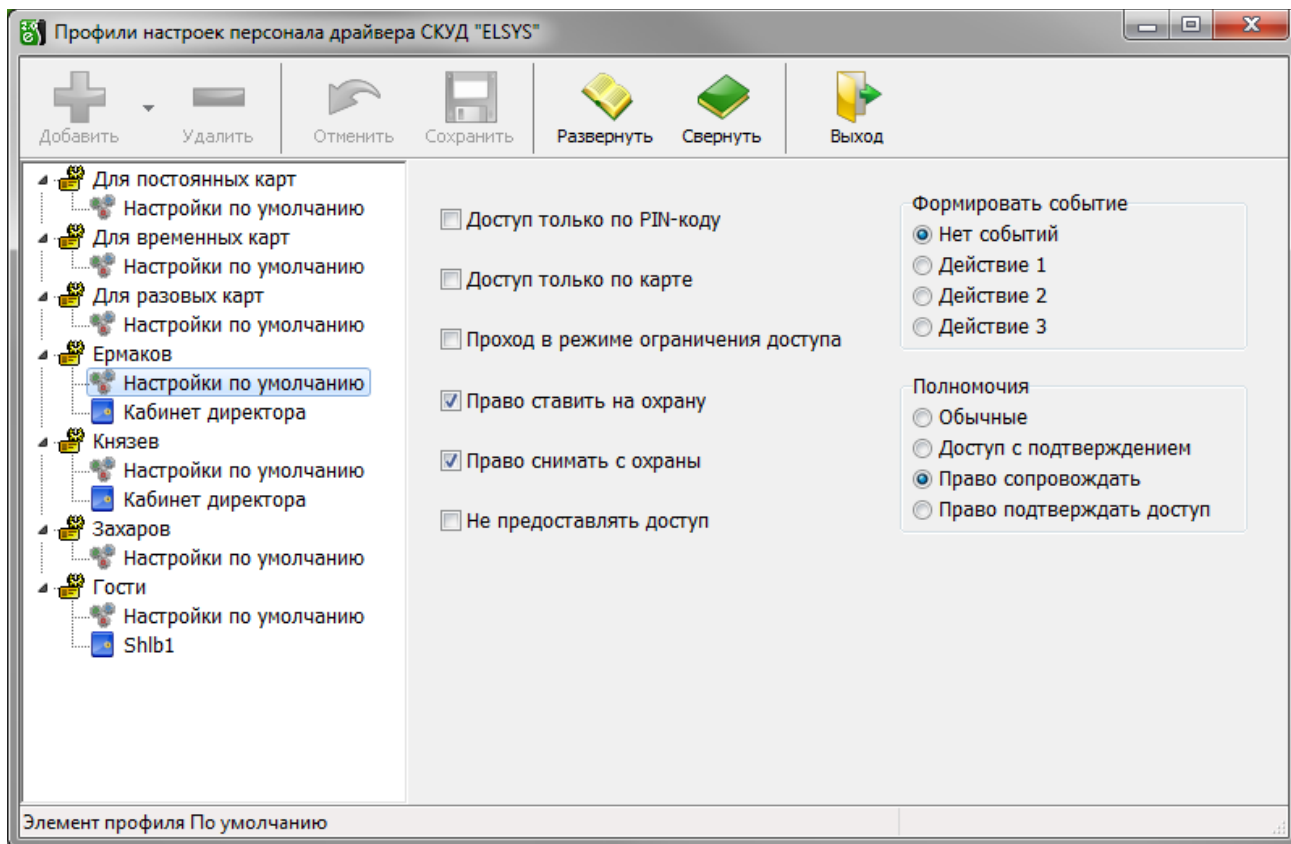


Рисунок 139 - Настройки профиля по умолчанию

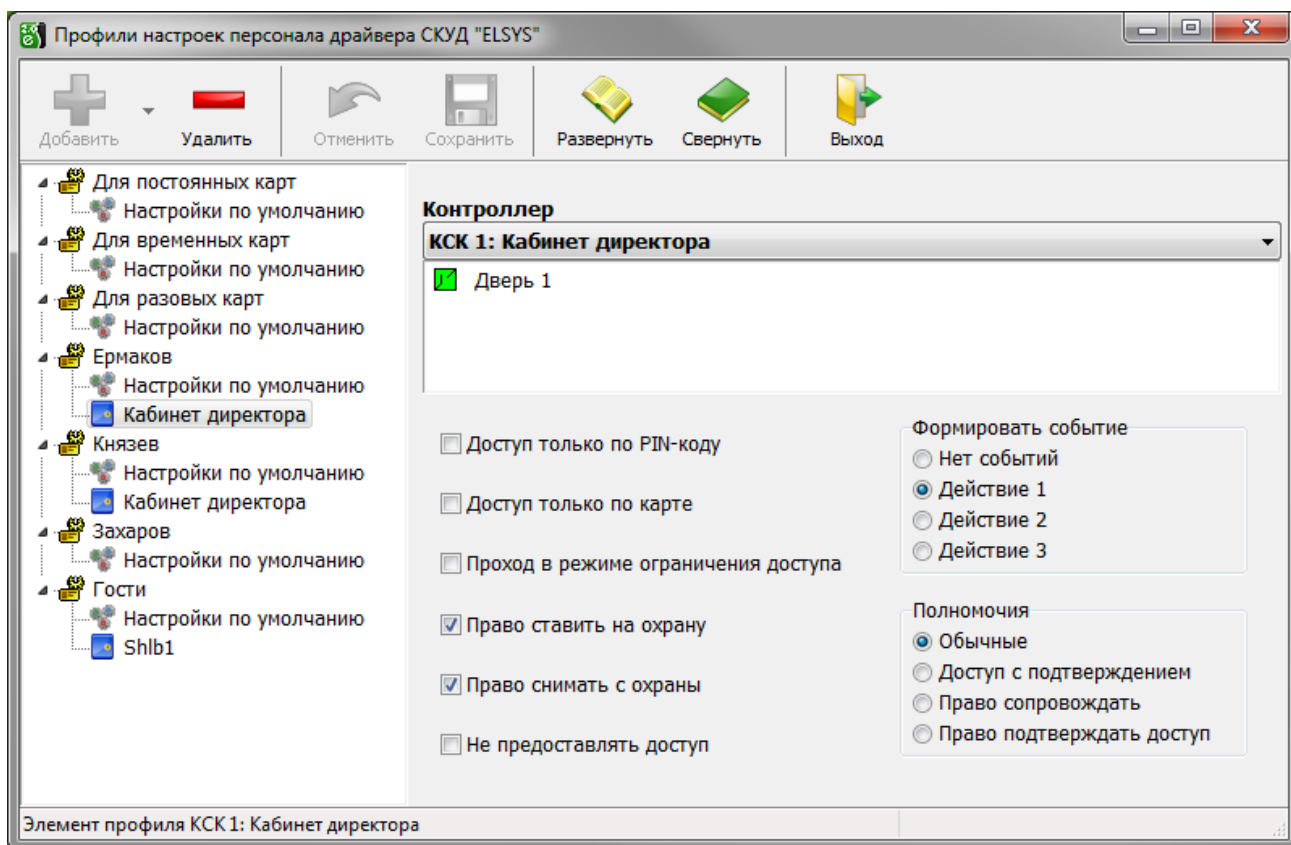


Рисунок 140 - Настройки элемента профиля

«**Проход в режиме ограничения доступа**» – эта настройка позволяет получать разрешение на проход, если считыватель находится в режиме ограничения доступа.

«**Право ставить на охрану**» и «**Право снимать с охраны**» – эти опции позволяют выполнять пользователю действия по управлению охраной с помощью кнопки управления охраной (см. п. 5.12, рисунок 75). Опция «**Право ставить на охрану**», кроме того, разрешает сотруднику использование служебных PIN-кодов (см. п. 9.1.6).

«**При предоставлении доступа формировать событие**» - если выбрано одно из событий (действие 1, действие 2, действие 3), то при предъявлении карты будут обрабатываться взаимодействия, назначенные на это событие считывателя.

«**Не предоставлять доступ**» - если эта опция включена, то карта может использоваться только для управления охраной и выполнения других действий. Доступ не предоставляется.

Группа настроек «**Полномочия**». По умолчанию – «**Обычные**». Если установлены полномочия «**Доступ с подтверждением**», то для предоставления доступа необходимо вслед за предъявлением данной карты предъявить карту с полномочиями «**Право сопровождать**» или «**Право подтверждать доступ**».

Различие между последними двумя полномочиями в том, что картам с полномочиями «**Право сопровождать**» при подтверждении доступа также предоставляется доступ (система фиксирует проход двух сотрудников), а картам с полномочиями «**Право подтверждать доступ**» - нет (будет зафиксирован проход первого сотрудника). Во всём

остальном права этих двух групп полномочий соответствуют полномочиям «Обычные». Если для считывателя включена опция «Подтверждать доступ для карт, требующих подтверждения», то для карт с полномочиями «Доступ с подтверждением» подтверждение осуществляется только кнопкой дежурного оператора «Подтверждение доступа».

Если назначенный пропуску профиль не имеет дочерних элементов, то для всех точек доступа, входящих в уровень доступа пропуска, действуют настройки профиля по умолчанию.

Если назначенный пропуску профиль содержит контроллеры, то для точек доступа подключенных к этим контроллерам и входящих в уровень доступа пропуска действуют настройки соответствующих контроллеров, для остальных точек доступа действуют настройки профиля по умолчанию.

В бюро пропусков по умолчанию для пропуска задаётся профиль в соответствии с его типом: для постоянных пропусков задаётся профиль «Для постоянных карт», для временных пропусков - профиль «Для временных карт», для разовых пропусков - профиль «Для разовых карт».

Изменить назначенный пропуску профиль можно в бюро пропусков, указав в свойствах пропуска на вкладке «Профили» заранее подготовленный в конфигураторе профилей требуемый профиль (рисунок **Ошибка! Источник ссылки не найден.**).

Назначаемые в бюро пропусков профили по-умолчанию можно изменить, выбрав в главном меню бюро пропусков пункт **«Инструменты -> Наборы пропусков...»** (рисунок 142). На рисунке 143 показано назначение разовым пропускам профиля «Гости».

При выходе из конфигуратора все внесённые изменения загружаются в контроллеры.

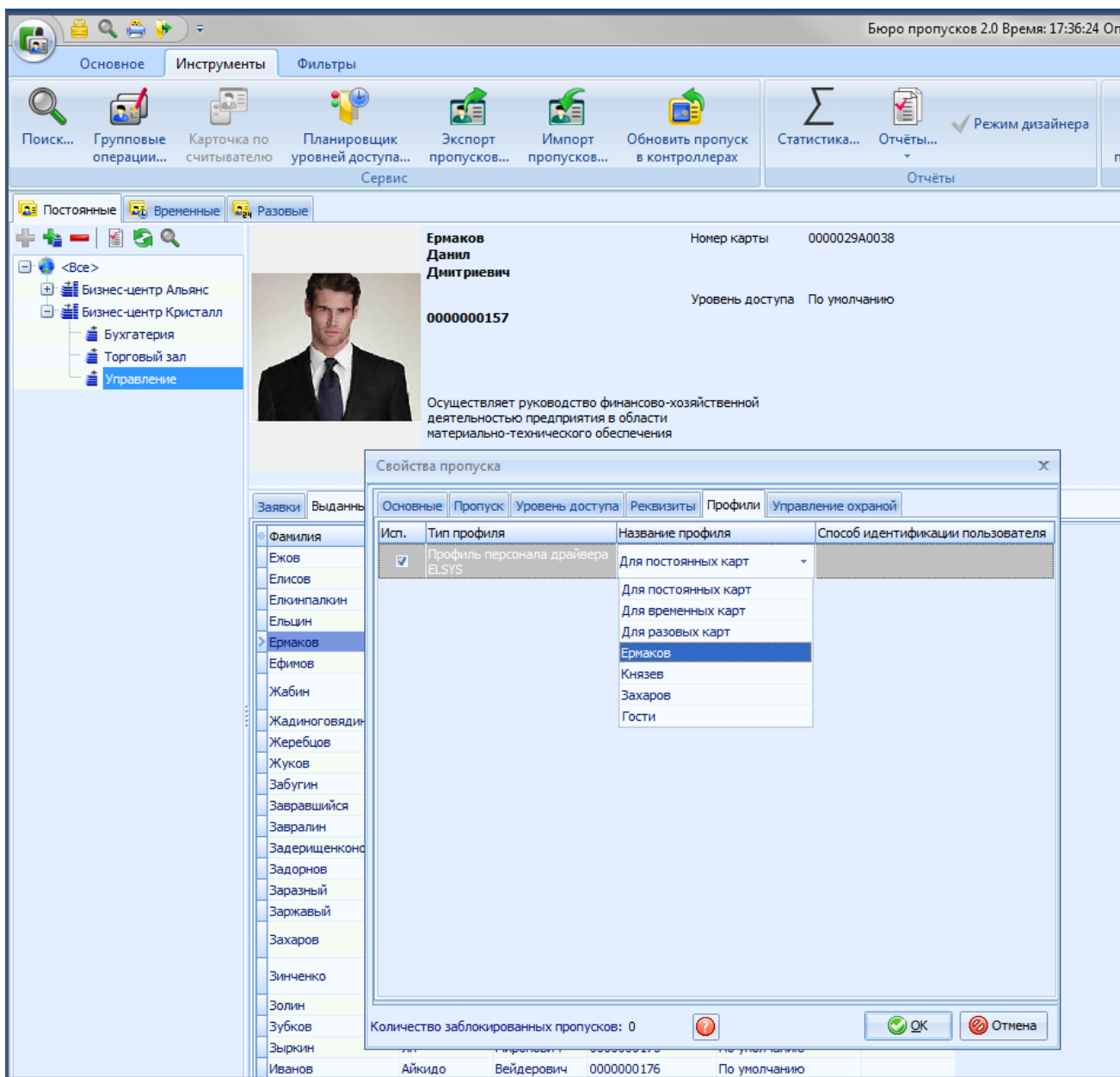


Рисунок 141 - Назначение пропуску персоны «Ермаков Данил Дмитриевич» профиля «Ермаков»

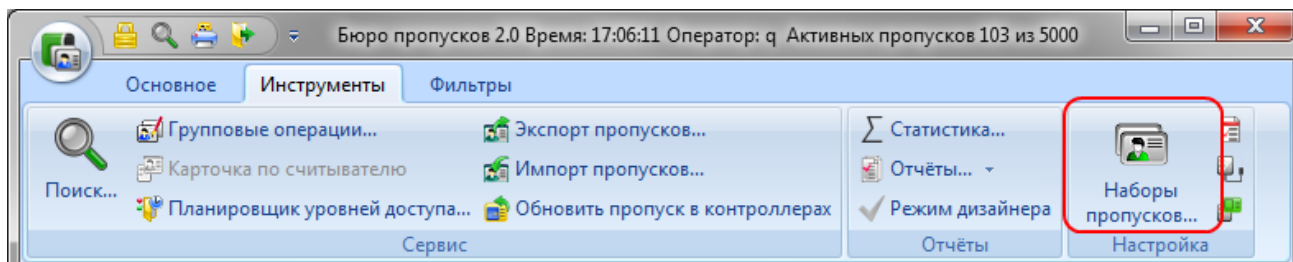


Рисунок 142 - Наборы пропусков



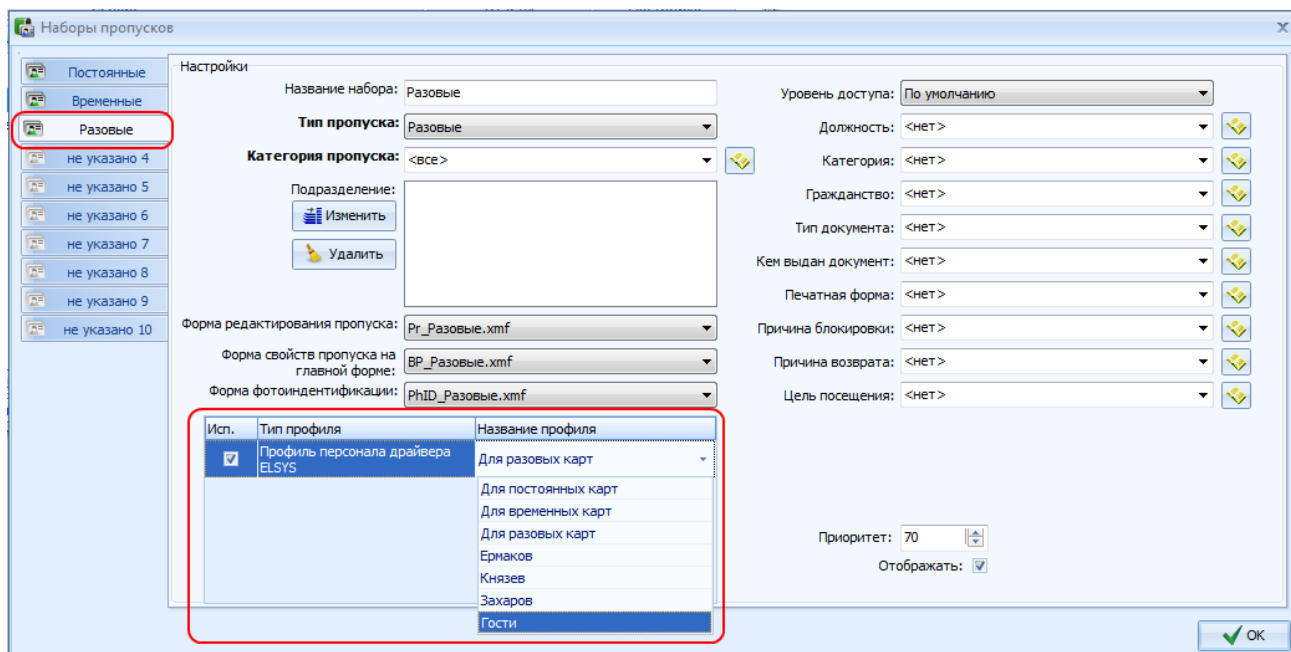


Рисунок 143 - Назначение профиля по-умолчанию «Гости» для разовых пропусков

### 9.3 Настройка автоматической постановки раздела на охрану при выходе последнего сотрудника

Для того, чтобы использовать эту функцию, необходимо включить одноимённую опцию раздела («Автоматическая постановка на охрану при выходе последнего сотрудника» на рисунке 69). Эта функция может быть включена только для одного раздела, содержащего в своем составе одну или две двусторонние двери. Если дверь, входящая в раздел, участвует в глобальном контроле последовательности прохода, необходимо выполнение следующих условий:

- для двери, входящей в раздел, должны быть настроены внешняя и внутренняя зоны доступа (при этом они не должны совпадать);
- во внутреннюю зону доступ должен осуществляться только через дверь (двери), входящую в раздел. Никакие другие точки доступа не должны граничить с внутренней зоной доступа, ни в этом, ни в других контроллерах.

Если глобальный контроль последовательности прохода в этом контроллере не используется никаких дополнительных настроек не нужно.

При использовании автоматической постановки последним выходящим сотрудником рекомендуется выполнить следующие настройки:

- для входного ШС (двери) установить задержку взятия;
- для остальных ШС, исключая объемные, установить опцию «Автоматическая постановка на охрану из состояния «Не взято» (рисунок 67);



- для раздела выключить настройку **«Ставить на охрану, если все зоны готовы»** (рисунок 69);
- включить настройку раздела **«Автоматическое снятие с охраны при входе в помещение»** (рисунок 69);
- включить настройку **«Досрочная постановка на охрану после выхода»** (это нужно, чтобы последний выходящий сотрудник успел проконтролировать, все ли ШС, входящие в раздел, поставлены на охрану, рисунок 69).

Такое сочетание настроек гарантирует автоматическую постановку раздела на охрану при любых состояниях охранных ШС и автоматическое снятие помещения с охраны при входе в помещение.

При использовании автоматической постановки на охрану подсчёт числа сотрудников в помещении будет выполняться после каждого события «Штатный вход» или «Штатный выход», зарегистрированного на двери, входящей в состав раздела. При подсчёте числа сотрудников учитывается текущее местоположение каждого пользователя, а не общее число событий «Штатный вход/выход» что существенно повышает точность подсчёта количества сотрудников.

При постановке раздела на охрану счётчик персонала автоматически сбрасывается (устанавливается в нуль). После снятия раздела с охраны контроллер после каждого прохода обновляет счётчик персонала. В момент выхода последнего сотрудника (соответствует моменту регистрации события «Штатный выход», формируемого одновременно с открыванием двери), осуществляется автоматическая постановка раздела на охрану. По истечении 5 с после закрывания двери (если включена настройка **«Досрочная постановка на охрану после выхода»**) выполнится досрочная постановка всех ШС раздела на охрану.

Если по истечении времени задержки взятия объёмные и входные ШС будут в нарушенном состоянии, будет сформирована тревога. Если ШС имеет включенную опцию **«Автоматическая постановка на охрану из состояния «Не взято»**, он в случае неготовности в момент постановки на охрану будет пребывать в состоянии «Невзятие» до тех пор, пока не восстановится его нормальное состояние. Поэтому, если по истечении 5 с после закрытия двери, раздел полностью не поставлен на охрану, сотрудник должен вручную снять раздел с охраны и устранить причину неготовности охранных ШС. Раздел должен быть снят с охраны до окончания времени задержки взятия входного ШС, в противном случае будет сформирована тревога. О наличии нарушенных ШС после выхода из помещения можно узнать по световой и звуковой индикации считывателей, а также по миганию светового оповещателя «Лампа».

Поставленный на охрану раздел снять с охраны имеют право только пользователи, имеющие полномочия «Снятие с охраны». Это условие актуально и в случае, если включена настройка **«Автоматическое снятие с охраны при входе в помещение»**. Для всех

остальных сотрудников, которым не назначены полномочия «Снятие с охраны», доступ в охраняемое помещение будет ограничен.

Следует помнить, что автоматическая постановка на охрану при выходе последнего выходящего сотрудника является функцией, повышающей удобство пользования системой, но не должна рассматриваться как единственный способ управления режимами охраны. Возможен ряд ситуаций, в которых необходимо вмешательство дежурного оператора или пользователя.

Некоторые из возможных ситуаций приведены в таблице 19.

**Таблица 19 – Описание ситуаций, требующих вмешательства дежурного оператора при автоматической постановке на охрану**

№	Описание ситуации	Причины	Способ решения
1	Контроллер считает, что выходит последний сотрудник, в то время как в помещении остались люди	Произошёл сбой при подсчёте людей по причине того, что кто-либо из находящихся в помещении вошёл без карты либо предъявил карту на выход, но не вышел (например, чтобы впустить посетителя, не имеющего карты). Помещение будет поставлено на охрану, а в помещении будут находиться все нарушители пропускного режима.	Поскольку в помещении остались люди, и они же являются нарушителями пропускного режима, ошибочная постановка помещения на охрану будет замечена. Необходимо снять помещение с охраны, в течение действия времени задержки взятия. И затем, при выходе последнего сотрудника, – вручную поставить помещение на охрану.
2	Вышел последний сотрудник, в то время как контроллер считает, что в помещении остались люди	Произошёл сбой при подсчёте людей по причине того, что кто-либо из сотрудников вышел вслед за другим, не отметившись на выходном считывателе. Либо (что менее вероятно) кто-либо предъявил карту на вход, открыл дверь, но не вошёл. Помещение не будет поставлено на охрану.	Если сотрудник, совершающий выход из помещения, точно знает, что больше в помещении никого нет, он должен вручную поставить помещение на охрану. По отсутствию характерной звуковой индикации на считывателе и световой – на оповещателе «Лампа», сотрудник должен определить, что отсутствовала попытка постановки на охрану.
3	Неудачная постановка на охрану при выходе последнего выходящего сотрудника	Неготовность охранных ШС в составе раздела	При выходе из помещения сотрудник, обнаружив, что выполняется автоматическая постановка на охрану, должен дождаться полной постановки раздела на охрану. Если по

**Таблица 19 – Описание ситуаций, требующих вмешательства дежурного оператора при автоматической постановке на охрану**

№	Описание ситуации	Причины	Способ решения
			истечении 5 с после закрытия двери раздел полностью не поставлен на охрану, сотрудник должен снять раздел с охраны, совершив вход в помещение, и устранить причину неготовности охранных ШС.

## 9.4 События драйвера «Бастион-2 – Elsys»

В этом разделе приведены все события драйвера «Бастион-2 – Elsys», которые используют контроллеры и компьютер в своей работе. Большинство событий регистрируются в буфере событий контроллера (некоторые из них – опционально), затем передаются по интерфейсу RS-485 и обрабатываются компьютером. Ниже описано участие событий во взаимодействиях и в записи в буфер событий. Более подробная информация о событиях приведена в «Руководстве по эксплуатации СКУД Elsys».

### 9.4.1 События выходов и групп выходов

События выходов перечислены в таблице 20.

**Таблица 20 - События выходов и групп выходов**

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Включение	Да	Да	События пишутся в буфер только при включенной опции «Мониторинг состояния выхода»
Выключение	Да	Да	
Окончание работы по формуле	Да	Да	Событие пишется в буфер только при включенной опции «Мониторинг окончания работы по формуле»

События выходов «Включение» и «Выключение» регистрируются в момент изменения состояния выхода, а событие «Окончание работы по формуле» - в момент окончания работы формулы (если работа выхода по формуле не была прервана командой «Включить» или «Выключить»). Взаимодействия на эти события обрабатываются всегда, независимо от того, включена их регистрация в буфере событий, или нет. Группы обладают всеми свойствами выхода и могут формировать те же события. Пустые группы можно использовать в разных вспомогательных целях.

#### 9.4.2 События точек доступа

Самый обширный список событий - у точек доступа (дверей и турникетов). Эти события можно разделить на три группы. Первая группа – события, фактически повторяющие события датчика прохода («Взлом», «Открытие двери», «Удержание двери» и т. д.), при этом соответствующие события датчика прохода не регистрируются в протоколе (однако, возможно назначение на них аппаратных взаимодействий). События этой группы приведены в таблице 21.

Последние четыре события формируются драйвером «Бастион-2 – Elsys» вместо сообщаемых контроллером событий «Штатный вход» и «Штатный выход», если им предшествовала одна из описанных ниже последовательностей событий: «Нарушение временной зоны» («Нарушение зоны доступа») и «Предоставление доступа» с одинаковым временем (с точностью до секунды).

**Таблица 21 - События, формируемые при срабатывании датчика прохода**

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Штатный вход (+ № карты)	Да	Да	
Штатный выход (+ № карты)	Да	Да	
Вход под принуждением (+ № карты)	Да	Да	
Выход под принуждением (+ № карты)	Да	Да	
Дверь не заперта	Да	Да	Только для дверей с электромеханическим замком
Взлом	Да	Да	
Удержание	Да	Да	
Закрытие двери	Да	Да	
Открывание двери	Да	Да	Используется для мониторинга состояния дверного контакта при разблокированной двери

Таблица 21 - События, формируемые при срабатывании датчика прохода

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
КЗ дверного контакта	Да	Да	При обработке взаимодействий – событие «Неисправность»
Обрыв дверного контакта	Да	Да	При обработке взаимодействий – событие «Неисправность»
Фактический выход по кнопке	Нет	Да	
Ворота закрыты	Да	Да	Только для ворот
Ворота приоткрыты	Да	Да	Только для ворот
Ворота открыты полностью	Да	Да	Только для ворот
Вход с нарушением временной зоны (+ № карты)	Нет	Нет	Формируется драйвером на основе предыстории событий вместо сообщаемого контроллером события «Штатный вход»
Выход с нарушением временной зоны (+ № карты)	Нет	Нет	Формируется драйвером на основе предыстории событий вместо сообщаемого контроллером события «Штатный выход»
Вход с нарушением зоны доступа (+ № карты)	Нет	Нет	Формируется драйвером на основе предыстории событий вместо сообщаемого контроллером события «Штатный вход»
Выход с нарушением зоны доступа (+ № карты)	Нет	Нет	Формируется драйвером на основе предыстории событий вместо сообщаемого контроллером события «Штатный выход»

Такая последовательность может быть сформирована лишь в случае, если используется «мягкий» режим доступа (т. е. для считывателей включена одна из опций «Предоставлять доступ при нарушении временной зоны» или «Предоставлять доступ при нарушении зоны доступа»). Для считывателя обязательно должна быть включена опция «Мониторинг предоставления доступа» (в противном случае событие «Предоставление доступа» не будет сформировано).

«Нарушение временной зоны» («Нарушение зоны доступа»), «Подтверждение доступа оператором», «Предоставление доступа» (последнее событие может отсутствовать, если

выключена опция «Мониторинг предоставления доступа»). Такая последовательность может быть сформирована, если используются контроллеры версий 1.37 (т. к. начиная с этой версии регистрируется событие «Подтверждение доступа оператором») и выше, а также используется режим с подтверждением доступа оператором.

Описанные выше события «Вход/Выход с нарушением ... » могут быть использованы при формировании отчётов о нарушителях режима доступа.

Вторая группа, самая многочисленная, – это события, связанные с предъявлением карты (большинство подобных событий имеются в двух вариантах – для входного и для выходного считывателя; полный текст этих событий содержит информацию о том, на каком считывателе, входном или выходном, произошло событие). Все эти события также содержат также номер карты или PIN-код. События этой группы приведены в таблице 22.

**Таблица 22 - События точек доступа, связанные с предъявлением карты доступа**

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Предоставление доступа	Да	Да	События записываются в буфер только при включенной опции «Мониторинг предоставления доступа»
Предоставление доступа под принуждением	Да	Да	
Нарушение зоны доступа	Да	Да	
Отказ в доступе - нет прав	Да	Да	
Нарушение временной зоны	Да	Да	
Неизвестная карта	Да	Да	
Неизвестный PIN-код	Да	Да	
Запрет доступа (ограничение доступа)	Да	Да	
Отказ в доступе – блокировка	Да	Да	
Неверный PIN-код	Да	Да	

Таблица 22 - События точек доступа, связанные с предъявлением карты доступа

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Отказ в доступе - нет полномочий	Да	Да	
Ошибка ввода второй карты	Да	Да	
Ошибка ввода третьей карты	Да	Да	
Любое нештатное событие	Да	Нет	
Предъявлена первая карта	Да	Нет	
Предъявлена вторая карта	Да	Нет	
Предъявлена третья карта	Да	Нет	
Действие 1	Да	Да	События записываются в буфер только при включенной опции «Мониторинг пользовательских безусловных действий»
Действие 2	Да	Да	
Действие 3	Да	Да	
Постановка на охрану	Да	Да	События записываются в буфер только при включенной опции «Мониторинг пользовательских условных действий». Событие записывается к кодом карты.
Снятие с охраны	Да	Да	
Требуется подтверждение доступа	Да	Да	События записываются в буфер только при включенной опции «Мониторинг предоставления доступа»
Подтверждение доступа оператором	Да	Да	В буфер событий записывается событие «Штатное предоставление доступа». Начиная с версии 1.37 контроллеры регистрируют также событие «Подтверждение доступа оператором»

Таблица 22 - События точек доступа, связанные с предъявлением карты доступа

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Отказ в доступе оператором	Да	Да	
Подтверждение доступа картой	Нет	Да	
Сброс режима подтверждения	Да	Нет	
Ввод PIN1..16 + PROX (вх. сч.)	Да	Да	16 событий, соответствующих отдельным действиям при вводе служебного PIN-кода и предъявлении карты
Ввод PIN1..16 + PROX (вых. сч.)	Да	Да	16 событий, соответствующих отдельным действиям при вводе служебного PIN-кода и предъявлении карты
Ввод пароля (вх. сч.)	Да	Нет	Ввод одного из 16 служебных PIN-кодов
Ввод пароля (вых. сч.)	Да	Нет	
Предъявление служебной карты (вх. сч.)	Да	Нет	
Предъявление служебной карты (вых. сч.)	Да	Нет	
Штатное предъявление служебной карты (вх. сч.)	Да	Нет	
Штатное предъявление служебной карты (вых. сч.)	Да	Нет	

И, наконец, третья группа – это события-команды для турникетов и ворот, используемые для задания специфичных для разных типов устройств алгоритмов. Список этих событий приведён в приведённых ниже таблицах 23 - 24.



Таблица 23 - События-команды для ворот

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Открыть	Да	Нет	
Закрыть	Да	Нет	
Стоп	Да	Нет	
Заблокировать	Да	Нет	

Таблица 24- События-команды для турникета

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Заблокировать вход	Да	Нет	
Заблокировать выход	Да	Нет	
Разблокировать вход	Да	Нет	
Разблокировать выход	Да	Нет	
Нормальный режим (вход)	Да	Нет	
Нормальный режим (выход)	Да	Нет	

### 9.4.3 События входов

События, регистрируемые на входах контроллеров Elsys-MB, приведены в таблице 25. Любой вход имеет четыре основных состояния («на охране», «норма – готов к постановке на охрану»; «тревога»/«неготовность шлейфа»). Соответственно, это две пары физических состояний цифрового входа, соответствующие режимам «На охране» и «Вне охраны». Опция **«Фиксировать тревогу»** должна быть включена, если предполагается использовать вход как охранный. В этом режиме тревожное состояние входа сохраняется до тех пор, пока не придёт команда («постановка на охрану» или «снятие с охраны»).

Таблица 25 - События входов

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Обрыв	Да	Да	Событие пишется в буфер только при включенной опции <b>«Мониторинг состояния входа»</b> . При обработке взаимодействий события «Обрыв» и «Короткое замыкание» интерпретируются как неисправность
Короткое замыкание	Да	Да	
Норма (готов к взятию на охрану)	Да	Да	События пишутся в буфер только при включенной опции <b>«Мониторинг состояния входа»</b>
Неготовность шлейфа	Да	Да	
На охране	Да	Да	
Тревога	Да	Да	
Удержание	Да	Да	
Невзятие на охрану	Да	Да	
Снятие с охраны	Да	Да	
Задержка взятия	Да	Да	
Задержка взятия - неготовность	Да	Да	
Задержка тревоги	Да	Да	
Неисправность	Да	Да	

Если опция «**Фиксировать тревогу**» выключена, состояние входа регистрируется в зависимости от того, на охране он или нет. Опция «Отслеживать состояние вне охраны» может быть выключена, если события о готовности/неготовности входа к постановке на охрану неинтересны и засоряют протокол (например, открытие/закрытие двери торгового центра в часы работы; то же, в ночные часы, если зона на охране – является тревогой). Если зона не готова к постановке на охрану, а производится попытка поставить вход на охрану, формируется событие «Не взятие».

#### 9.4.4 События контроллеров

События, относящиеся к устройству «Контроллер», приведены в таблице 26.

**Таблица 26 - События контроллеров**

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Выключение питания	Нет	Да	
Включение питания	Нет	Да	
Очистка конфигурации	Нет	Да	
Разрушение БД контроллера	Нет	Да	
Сброс программный	Да	Да	
Сброс аппаратный	Нет	Да	
Авария первичного электропитания	Нет	Да	
Восстановление первичного электропитания	Нет	Да	
Взлом корпуса	Нет	Да	
Восстановление зоны контроля взлома	Нет	Да	
Потеря связи	Нет	Нет	События формируются драйвером «Бастион-2 – Elsys»
Восстановление связи	Нет	Нет	
Сброс антипассбэка	Нет	Нет	
Инициализация	Нет	Нет	
Ошибка в процессе инициализации	Нет	Нет	
Аккумулятор в норме	Нет	Да	
Аккумулятор разряжен	Нет	Да	

Таблица 26 - События контроллеров

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Включение режима MASTER-SLAVE	Нет	Да	
Включение режима MULTIMASTER	Нет	Да	
Включение режима UDP	Нет	Да	
Выключение режима UDP	Нет	Да	
Восстановление буфера событий	Нет	Да	
Частичное восстановление буфера событий	Нет	Да	
Восстановление связи между Elsys-MB и Elsys-IP	Нет	Да	
Нет связи между Elsys-MB и Elsys-IP	Нет	Да	
Отсутствует модуль расширения памяти	Нет	Да	
Некорректный номер временного блока	Нет	Нет	События формируются драйвером «Бастион-2 – Elsys»
Некорректный номер уровня доступа	Нет	Нет	
Превышено допустимое количество временных зон	Нет	Нет	
Превышено допустимое количество постоянных карт	Нет	Нет	
Превышено допустимое количество уровней доступа	Нет	Нет	
Срабатывание сторожевого таймера	Нет	Да	

На событие «Сброс» (взаимодействия на него обрабатываются в момент сброса или включения питания) может быть назначен ряд действий, приводящих в исходное состояние все устройства (выходы – включить, входы – взять под охрану, двери – вернуть в нормальный режим и т. п. ).

Сообщение о потере связи с контроллером генерируется компьютером в том случае, если несколько раз подряд контроллер не передавал очередных сообщений.

Сообщение о восстановлении связи генерируется в следующих случаях:

- а) установка связи с одним из контроллеров, занесенных в базу данных драйвера;
- б) запуск программы;
- в) вход в программу под другим именем.

Кроме того, сообщения о потере и восстановлении связи генерируются при выходе из конфигуратора оборудования. Это связано с тем, что в этот момент драйвер временно приостанавливает обмен с контроллерами и перечитывает конфигурацию оборудования из базы данных.

Ряд событий, используемых при настройке взаимодействий, и формально относящихся также к устройству «Контроллер», описаны в таблице 27. Их использование подробно описано в п. 9.1.

**Таблица 27- Дополнительные события**

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Начало временного блока	Да	Нет	Доп. параметр - № врем. блока (1..125)
Окончание временного блока	Да	Нет	Доп. параметр - № врем. блока (1..125)
Активность логической формулы	Да	Нет	Доп. параметр - № логической формулы (1..20)
Неактивность логической формулы	Да	Нет	Доп. параметр - № логической формулы (1..20)
Восстановление связи с другим контроллером	Да	Нет	Доп. параметр – адрес контроллера (0 – компьютер, 64 – все контроллеры)
Потеря связи с другим контроллером	Да	Нет	Доп. параметр – адрес контроллера (0 – компьютер, 64 – все контроллеры)
Сообщение от контроллера	Да	Нет	Доп. параметры – адрес контроллера (64 – любой контроллер) и № сообщения (1..64)
Счётчик (POSTDEC) равен значению	Да	Нет	Доп. параметры - № счётчика (1..8) и значение (0..63)
Счётчик (POSTINC) равен значению	Да	Нет	Доп. параметры - № счётчика (1..8) и значение (0..63)

Таблица 27- Дополнительные события

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Счётчик равен значению	Да	Нет	Доп. параметры - № счётчика (1..8) и значение (0..63)

#### 9.4.5 События разделов

События разделов приведены в таблице 28.

Таблица 28 – События разделов

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Взятие на охрану	Да	Да	События пишутся в буфер только при включенной опции в свойствах раздела <b>«Протоколировать события»</b>
Взятие на охрану с задержкой	Да	Да	
Невзятие на охрану	Да	Да	
Снятие с охраны	Да	Да	
Тревога	Да	Да	
Тревога входной зоны	Да	Да	

#### 9.4.6 События сетевых контроллеров Elsys-MB-Net

События, формируемые сетевыми контроллерами Elsys-MB-Net, приведены в таблице 29.

Таблица 29 - События, формируемые контроллерами Elsys-MB-Net

Событие	Комментарий
Включение режима MULTIMASTER	Формируется КСК Elsys-MB-Net в момент включения режима «MULTIMASTER»
Включение режима MASTER-SLAVE	Формируется КСК Elsys-MB-Net в момент включения режима «MASTER-SLAVE»
Срабатывание сторожевого таймера	Формируется в случае сброса КСК Elsys-MB-Net по сторожевому таймеру

Таблица 29 - События, формируемые контроллерами Elsys-MB-Net

Событие	Комментарий
Сброс программный	Формируется в случае сброса КСК Elsys-MB-Net по внешней команде
Сброс аппаратный	Формируется в случае сброса КСК Elsys-MB-Net кнопкой RESET
Разрушение БД контроллера	Формируется в случае обнаружения сетевым контроллером ошибок во внутренней базе данных. Необходимо выяснить, почему это произошло, и проинициализировать такой контроллер.
Потеря связи	Формируется драйвером в случае разрыва IP-соединения с КСК Elsys-MB-Net
Восстановление связи	Формируется драйвером в случае восстановления IP-соединения с КСК Elsys-MB-Net
Включение питания	Формируется КСК Elsys-MB-Net в момент включения сетевого питания
Выключение питания	Формируется КСК Elsys-MB-Net в момент выключения сетевого питания
Включение режима UDP	Формируется КСК Elsys-MB-Net в момент включения режима UDP
Выключение режима UDP	Формируется КСК Elsys-MB-Net в момент выключения режима UDP
Инициализация контроллера	Формируется драйвером в момент старта инициализации
Ошибка в процессе инициализации	Формируется драйвером при наличии ошибок инициализации

#### 9.4.7 События, формируемые драйвером «Бастион-2 – Elsys»

События, формируемые драйвером «Бастион-2 – Elsys», приведены в таблице 30.

Таблица 30 - События, формируемые драйвером «Бастион-2 – Elsys»

Событие	Комментарий
Включение режима MULTIMASTER	Регистрирует драйвер «Бастион-2 – Elsys» в момент включения режима «MULTIMASTER»

Включение режима MASTER-SLAVE	Регистрирует драйвер «Бастион-2 – Elsys» в момент включения режима «MASTER-SLAVE»
-------------------------------	---

#### 9.4.8 События биометрических считывателей

При использовании биометрических считывателей в составе СКУД Elsys могут приходиться тревожные события, связанные с идентификацией под принуждением и несанкционированным доступом к биометрическому считывателю (см. Таблица 31).

**Таблица 31 – События биометрических считывателей**

Событие	Комментарий
Идентификация под принуждением	Событие формируется при идентификации сигнатуры, для которой при записи в считыватель был установлен флаг принуждения. Если код карты, связанный с этой сигнатурой найден в базе данных бюро пропусков, то в событии также указывается фамилия и имя персоны.
Взлом корпуса	В зависимости от типа тампера биометрического считывателя событие формируется при съёме верхней панели корпуса или демонтаже считывателя.
Запущена полная инициализация	Формируется при запуске инициализации биометрического считывателя из окна управления биометрическими считывателями
Инициализация завершена успешно	Формируется после успешного окончания инициализации биометрического считывателя
Инициализация завершена с ошибками	Формируется после окончания процесса инициализации, в процессе которого возникли ошибки связи со считывателем или который был прерван пользователем.

#### Команды контроллеров Elsys-MB

В таблице 32 приведены все команды, которые можно выполнить (сообщить контроллерам по интерфейсу RS-485), во-первых, из контекстных меню или вкладки «Управление» конфигуратора оборудования, а, во-вторых, с помощью предварительно настроенных аппаратных взаимодействий.

**Таблица 32 - Команды контроллеров Elsys-MB**

Устройство	Команда	Диапазон значений аргументов
Вход	Поставить на охрану	0
	Поставить на охрану с задержкой	Интервал времени: 1..127 с



Таблица 32 - Команды контроллеров Elsys-MB

Устройство	Команда	Диапазон значений аргументов
	Снять с охраны	0
	Снять с охраны на интервал времени	Интервал времени: 1..127 с
<b>Выход</b>	Включить	
	Выключить	
	Переключить состояние на противоположное	
	Включить по формуле	Номер формулы: 0..15
<b>Дверь</b>	Открыть	
	Заблокировать	
	Нормальный режим	
	Разблокировать	
<b>Считыватель</b>	Заблокировать	0
	Заблокировать на интервал времени	Интервал времени: 1..63 с
	Снять блокировку	0
	Снять блокировку на интервал времени	Интервал времени: 1..63 с
	Ограничить доступ	
	Снять ограничение доступа	
<b>Турникет</b>	Открыть на вход	
	Заблокировать на вход	
	Нормальный режим (вход)	
	Разблокировать на вход	
	Открыть на выход	
	Заблокировать на выход	
	Нормальный режим (выход)	
	Разблокировать на выход	

Таблица 32 - Команды контроллеров Elsys-MB

Устройство	Команда	Диапазон значений аргументов
Ворота	Открыть	
	Закрыть	
	Стоп	
	Заблокировать	
	Нормальный режим	
Контроллер	Сформировать сообщение всем контроллерам	Адрес контроллера: 0, № сообщения: 1..64
	Сформировать сообщение контроллеру	Адрес контроллера: 1..63, № сообщения: 1..64
	Инкремент счётчика	№ счётчика: 1..8
	Декремент счётчика	№ счётчика: 1..8
	Установить значение счётчика	№ счётчика: 1..8, значение счетчика: 0..63
	Сбросить счётчик персонала	
	Сбросить счётчик персонала для УД	Номер УД: 1.. 16382

## 9.5 Индикация состояния устройств и разделов на планах


Устройства, входящие в состав СКУД Elsys, могут быть представлены на графическом плане объекта в виде пиктограмм, многоугольников (охранные зоны), ломаных линий (периметр). Эти элементы отображают текущее состояние устройств, а также позволяют выполнять команды управления из контекстного меню.

Различным устройствам соответствует свой набор состояний пиктограмм. Состояния пиктограмм формируются драйвером «Бастион-2 – Elsys» на основе предыстории событий, действий оператора и других данных, сообщённых оборудованием.






Если включен режим **«Подтверждение тревожных состояний оператором»** (см. рисунок 17), драйвер формирует состояние пиктограммы на основе неподтверждённых тревожных событий (к ним относятся сообщения о тревогах и

неисправностях). В этом режиме, даже если тревожная ситуация прекратилась, вид пиктограммы будет определяться неподтверждённым тревожным событием. Если таких событий было несколько, вид пиктограммы выбирается в соответствии с наиболее приоритетным состоянием. Если все тревожные события подтверждены, состояние пиктограммы отображает реальное состояние устройства.

**Внимание!** При использовании режима «Подтверждение тревожных состояний оператором» необходимо обеспечить отображение тревожных событий хотя бы на одном из постов «Бастион-2», иначе будет невозможно подтвердить тревожное состояние.

В таблицах 33 - 38 приведён набор состояний пиктограмм и их вид для устройств драйвера «Бастион-2 – Elsys». Значком  обозначены пиктограммы, которые находятся в мигающем режиме.

**Таблица 33 – Состояния устройств «контроллер», «КСК»**

Состояние	Вид пиктограммы контроллера	Вид пиктограммы КСК	Описание	Приоритет тревожного состояния
Норма			Устройство исправно	
Неисправность			Отсутствие связи или неисправность (например: авария сетевого питания, разряд аккумулятора)	1
Тревога			Взлом корпуса	2
<b>Примечание</b> – КСК не имеют датчика взлома, поэтому состояние «Тревога» для этих устройств не регистрируется				

**Таблица 34 – Состояния дверей**



Состояние	Вид пиктограммы	Описание	Приоритет тревожного состояния
Норма		Дверь закрыта	
Заблокировано		Дверь заблокирована. Доступ по предъявлению карты запрещён	

Таблица 34 – Состояния дверей








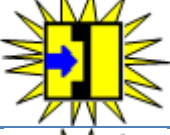


Состояние	Вид пиктограммы	Описание	Приоритет тревожного состояния
Разблокировано, дверь закрыта		Дверь разблокирована, находится в закрытом состоянии (датчик прохода замкнут)	
Разблокировано, дверь открыта		Дверь разблокирована, находится в открытом состоянии (датчик прохода разомкнут)	
Осуществление входа		Дверь в открытом состоянии. Состояние регистрируется после события «Штатный вход»	
Осуществление выхода		Дверь в открытом состоянии. Состояние регистрируется после события «Штатный выход»	
Дверь открыта		Дверь в открытом состоянии после выполнения команды «Открыть» и в иных случаях, когда направление прохода определить невозможно.	
Доступ разрешён, дверь закрыта		Дверь отперта, но находится в закрытом состоянии (датчик прохода замкнут). Состояние регистрируется после предоставления доступа по карте или выполнения команды «Открыть»	
<i>Попытка нештатного входа</i>		Было зарегистрировано нештатное предъявление карты при входе	1
<i>Попытка нештатного выхода</i>		Было зарегистрировано нештатное предъявление карты при выходе	2
Удержание двери		Дверь открыта, а время, отводимое на проход, истекло	3
<i>Дверь не заперта</i>		Дверь отперта, так как не был совершён проход. Состояние возможно только для дверей с электромеханическими замками-защёлками	4

Таблица 34 – Состояния дверей




Состояние	Вид пиктограммы	Описание	Приоритет тревожного состояния
<i>Вход под принуждением</i>		Было зарегистрировано событие «Предоставление доступа на вход под принуждением»	5
<i>Выход под принуждением</i>		Было зарегистрировано событие «Предоставление доступа на выход под принуждением»	6
Взлом		Дверь была открыта нештатным образом	7
<b>Примечание</b> - состояния, выделенные курсивом, формируются, только если включен режим «Подтверждение тревог оператором»			

Таблица 35 – Состояния ворот (шлагбаумов)











Состояние	Вид пиктограммы для ворот	Вид пиктограммы для шлагбаума	Описание	Приоритет тревожного состояния
Норма			Закрето	
Заблокировано			Ворота заблокированы. Доступ по предъявлению карты запрещён	
Полуоткрыто			Ворота частично открыты. Состояние регистрируется в процессе штатного открывания ворот. Для регистрации состояния необходимо наличие датчика закрытого состояния и датчика открытого состояния.	
Открыто			Ворота полностью открыты. Состояние регистрируется после штатного открывания ворот	
<i>Попытка нештатного входа</i>			Было зарегистрировано нештатное предъявление карты при входе	1

Таблица 35 – Состояния ворот (шлагбаумов)

Состояние	Вид пиктограммы для ворот	Вид пиктограммы для шлагбаума	Описание	Приоритет тревожного состояния
<i>Попытка нештатного выхода</i>			Было зарегистрировано нештатное предъявление карты при выходе	2
<i>Вход под принуждением</i>			Было зарегистрировано событие «Предоставление доступа на вход под принуждением»	5
<i>Выход под принуждением</i>			Было зарегистрировано событие «Предоставление доступа на выход под принуждением»	6
Взлом			Ворота были открыты нештатным образом	7
<b>Примечание</b> - состояния, выделенные курсивом, формируются, только если включен режим «Подтверждение тревог оператором»				

Таблица 36 – Состояния турникетов

Состояние	Вид пиктограммы	Описание	Приоритет тревожного состояния
Норма		Турникет закрыт (нормальный режим работы)	
Заблокировано		Турникет заблокирован на вход и на выход	
Разблокировано		Турникет разблокирован на вход и на выход	
Разблокировано на вход		Турникет разблокирован на вход, в направлении выхода работает в обычном режиме	
Разблокировано на выход		Турникет разблокирован на выход, в направлении входа работает в обычном режиме	

Таблица 36 – Состояния турникетов








Состояние	Вид пиктограммы	Описание	Приоритет тревожного состояния
Заблокировано на вход		Турникет заблокирован на вход, в направлении выхода работает в обычном режиме	
Заблокировано на выход		Турникет заблокирован на выход, в направлении входа работает в обычном режиме	
Разблокировано на вход, заблокировано на выход		Турникет разблокирован на вход, заблокирован на выход	
Заблокировано на вход, разблокировано на выход		Турникет заблокирован на вход, разблокирован на выход	
Осуществление входа		Турникет в открытом состоянии. Состояние регистрируется после события «Штатный вход» или выполнения команды «Открыть на вход»	
Осуществление выхода		Турникет в открытом состоянии. Состояние регистрируется после события «Штатный выход» или выполнения команды «Открыть на выход»	
Осуществление прохода		Турникет в открытом состоянии (для случаев, когда направление прохода определить невозможно)	
<i>Попытка нештатного входа</i>		Было зарегистрировано нештатное предъявление карты при входе	1
<i>Попытка нештатного выхода</i>		Было зарегистрировано нештатное предъявление карты при выходе	2
Удержание		Датчик прохода в нарушенном состоянии, а время, отводимое на проход, истекло. Применительно к	3

Таблица 36 – Состояния турникетов




Состояние	Вид пиктограммы	Описание	Приоритет тревожного состояния
		турникету это состояние означает, что поворотный механизм турникета удерживается в промежуточном положении	
<i>Вход под принуждением</i>		Было зарегистрировано событие «Предоставление доступа на вход под принуждением»	5
<i>Выход под принуждением</i>		Было зарегистрировано событие «Предоставление доступа на выход под принуждением»	6
Взлом		Турникет был открыт нештатным образом	7
<b>Примечание</b> - состояния, выделенные курсивом, формируются, только если включен режим "Подтверждение тревог оператором"			














Таблица 37 – Состояния выходов и групп выходов

Состояние	Вид пиктограммы	Описание
Включено		Управляющий выход включен
Выключено		Управляющий выход выключен

В таблице 38 приведены списки возможных состояний для пиктограмм охранных зон (входов) и разделов. Для этих устройств не применяется программный механизм подтверждения тревог, так как тревожные состояния формируются аппаратно. Для сброса тревоги в охранной подсистеме необходимо выполнить для охранной зоны или для раздела команду снятия с охраны или постановки на охрану.



Таблица 38 – Состояния входов и разделов

Состояние	Вид пиктограммы входа общего назначения	Вид пиктограммы охранного входа	Вид пиктограммы раздела	Описание
Снято с охраны				Состояние регистрируется, если вход или раздел снят с охраны и находится в состоянии «Норма – готовность к постановке на охрану»
На охране				Вход или раздел находится на охране или в состоянии «Задержка взятия - готовность»
Неготовность к постановке на охрану				Вход или раздел снят с охраны и находится в состоянии «Неготовность к постановке на охрану»
Тревога				Вход или раздел находятся в состоянии «Тревога» или «Задержка тревоги»
Неисправность				Состояние может быть зафиксировано только для тревожных входов, при регистрации короткого замыкания или обрыва
<b>Примечание</b> – Для охранных входов при настройке системы может быть задан иной вид пиктограмм и тип устройства				

## 9.6 Порты протоколов TCP/IP и UDP/IP, используемые КСК Elsys-MB-Net и контроллерами Elsys-MB-IP

Информация, приведённая в настоящей главе, может потребоваться для настройки системы, если в локальной сети используются брандмауэры или сетевые экраны.

Структурная схема, иллюстрирующая взаимодействие КСК Elsys-MB-Net и контроллеров Elsys-MB-IP между собой и с программным обеспечением «Бастион-2» изображена на рисунке 144.

В таблице 39 перечислены порты протоколов TCP/IP и UDP/IP, используемые коммуникационными сетевыми контроллерами Elsys-MB-Net.

В таблице 40 перечислены порты протокола UDP/IP, используемые модулями Elsys-IP при обмене данными.

Все порты, перечисленные в таблицах 39 - 40, должны быть разрешены для свободного обмена данными.

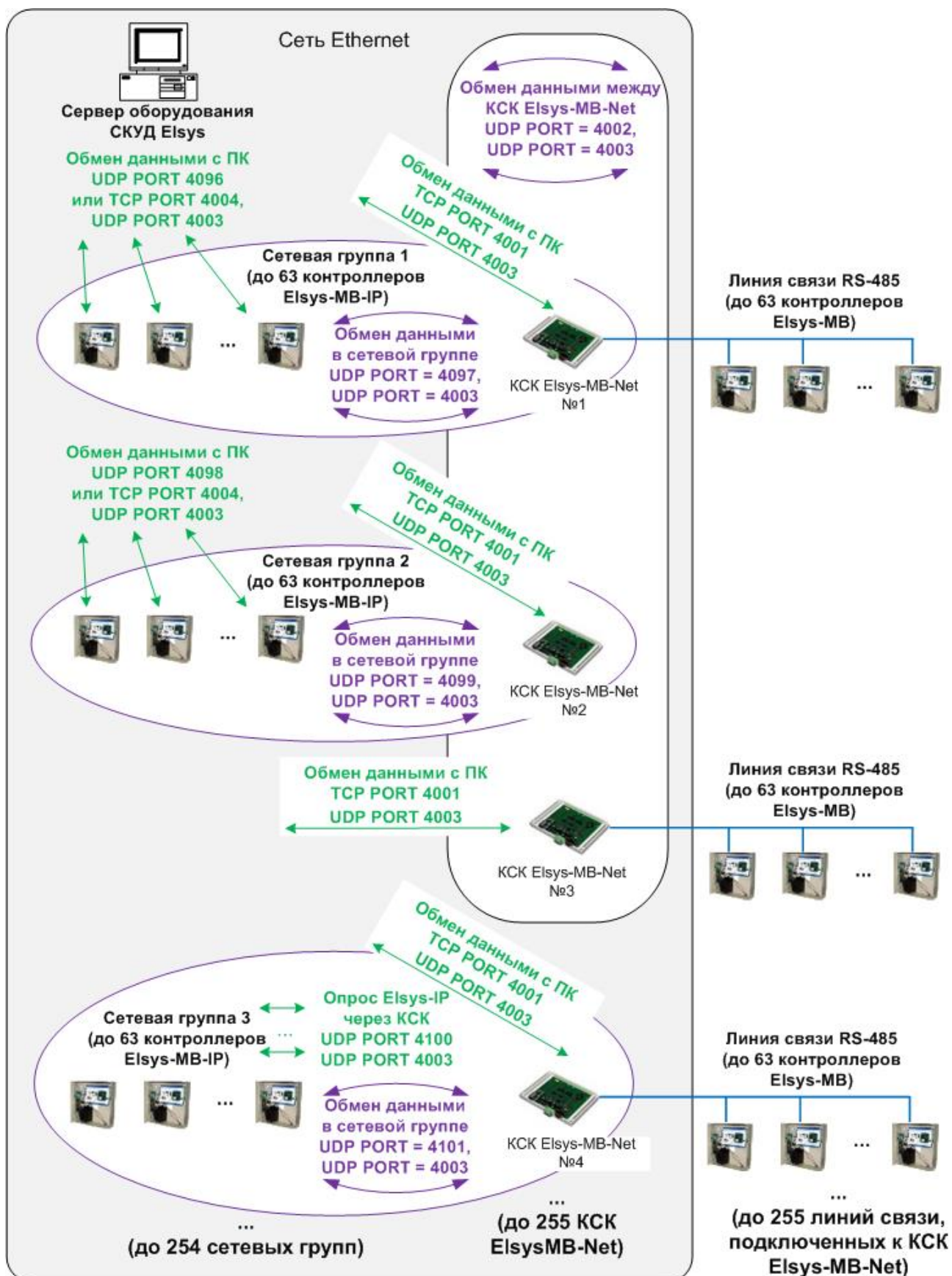


Рисунок 144 - Организация информационного обмена в СКУД Elsys с участием KCK Elsys-MB-Net и контроллеров Elsys-IP

Таблица 39 – Порты протоколов TCP/IP и UDP/IP, используемые КСК Elsys-MB-Net

№ порта	Тип порта	Назначение порта
4001	TCP	Используется для обмена данными между управляющим ПО и КСК Elsys-MB-Net. КСК является TCP-сервером, ПК – TCP-клиентом. КСК поддерживает только одно TCP-соединение
4002	UDP	Используется для обмена данными между КСК для обеспечения функции «Глобальный контроль последовательности прохода». По этому порту могут, в зависимости от режима работы, передаваться адресные и широковещательные UDP-дейтаграммы (с широковещательным адресом 255.255.255.255 или с адресом подсети).
4003	UDP	Используется для обмена широковещательными дейтаграммами с ПК при поиске оборудования и назначении сетевых настроек, а также для проверки связи с другими КСК Elsys-MB-Net и контроллерами Elsys-MB-IP.
4004	UDP	<i>Не используется (использовался в версиях КСК Elsys-MB-Net ниже 2.08 для проверки связи с другими КСК)</i>
$4096 + (N - 1) * 2 + 1$	UDP	Порт используется для обмена данными с контроллерами Elsys-MB-IP, если КСК включён в сетевую группу. По этому порту могут, в зависимости от режима работы, передаваться адресные и широковещательные (с широковещательным адресом 255.255.255.255 или с адресом подсети) UDP-дейтаграммы. Номер порта вычисляется по указанной формуле, где N – номер сетевой группы. Так, для сетевой группы 1 будет использоваться порт 4097, для сетевой группы 2 – 4099, для сетевой группы 10 – порт 4115 и т. д.

Таблица 40 – Порты протокола UDP/IP, используемые модулем Elsys-IP

№ порта	Назначение порта
$4096 + (N - 1) * 2$	Порт используется для обмена данными между управляющим ПО и контроллерами Elsys-MB-IP. По этому порту передаются адресные UDP-дейтаграммы. Номер порта вычисляется по указанной формуле, где N – номер сетевой группы. Так, для сетевой группы 1 будет использоваться порт 4096, для сетевой группы 2 – 4098, для сетевой группы 10 – порт 4114 и т. д.

Таблица 40 – Порты протокола UDP/IP, используемые модулем Elsys-IP

№ порта	Назначение порта
$4096 + (N - 1) * 2 + 1$	Порт используется для обмена данными между контроллерами Elsys-MB-IP. По этому порту могут, в зависимости от режима работы, передаваться адресные и широковещательные (с широковещательным адресом 255.255.255.255 или с адресом подсети) UDP-дейтаграммы. Номер порта вычисляется по указанной формуле, где N – номер сетевой группы. Так, для сетевой группы 1 будет использоваться порт 4097, для сетевой группы 2 – 4099, для сетевой группы 10 – порт 4115 и т. д.
4003	Используется для обмена широковещательными дейтаграммами с ПК при поиске оборудования и назначении сетевых настроек, а также для проверки связи с другими контроллерами Elsys-MB-IP и КСК Elsys-MB-Net.

## 10 Окно «Биометрия»

Окно работы с биометрическими считывателями вызывается с помощью кнопки «Биометрия», расположенной на ленте управления драйвером (рисунок 2).

Режим работы с биометрическими считывателями обеспечивает выполнение следующих функций:

- получение текущего состояния биометрических считывателей;
- получение системной информации о биометрических считывателях;
- проверку конфигурации биометрических считывателей;
- инициализацию биометрических считывателей.

Окно работы с биометрическими считывателями содержит список всех биометрических считывателей, подключенных к контроллерам доступа СКУД Elsys, в табличном виде (Рисунок 145).

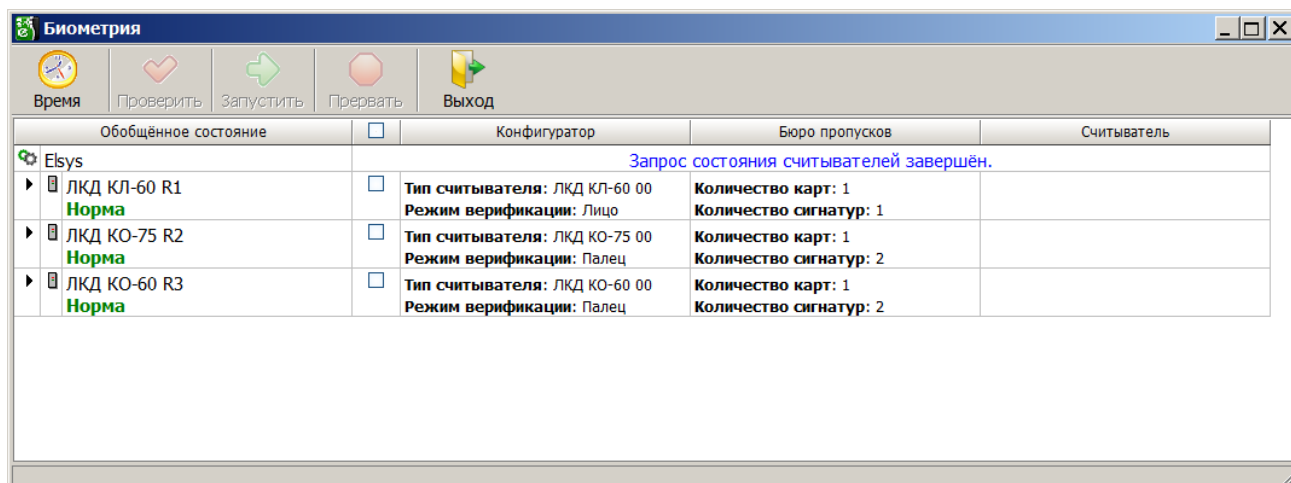


Рисунок 145 - Окно «Биометрия»






При открытии окна автоматически выполняется запрос текущего состояния всех биометрических считывателей, результаты которого отображаются в первом столбце таблицы.

Столбцы «Конфигуратор» и «Бюро пропусков» отображают данные конфигурации контроллеров, полученные от менеджера устройств и менеджера персонала, соответственно.

В столбце «Считыватель» отображается системная информация, полученная от биометрического считывателя при выполнении проверки конфигурации.

Назначение элементов на панели управления окна «Биометрия» представлено в таблице 41.

**Таблица 41 - Назначение элементов на панели управления окна «Биометрия»**

Элемент управления	Назначение
 Время	Кнопка служит для выполнения синхронизации даты и времени во всех биометрических считывателях, с которыми установлена связь.
 Проверить	Кнопка служит для запуска проверки конфигурации биометрических считывателей. Проверка конфигурации запускается автоматически после успешного завершения инициализации.
 Запустить	Кнопка служит для запуска инициализации биометрических считывателей.
 Прервать	Кнопка служит для прерывания длительных процессов запроса состояний, проверки конфигурации и инициализации, в случае потери связи со считывателями.
 Выход	Кнопка служит для закрытия окна «Биометрия»

Перед запуском системы в эксплуатацию необходимо проинициализировать полностью все считыватели. В дальнейшем все изменения в базе данных бюро пропусков (карты доступа, сигнатуры) должны загружаться автоматически, при этом инициализация не требуется. Исключением являются ошибки инициализации при доставке изменений из бюро пропусков, например, в случае отсутствия связи со считывателями, а также случаи больших изменений в базе данных бюро пропусков.

Инициализация может быть выполнена оператором АПК «Бастион-2», для профиля которого установлено разрешение «Инициализация биометрических считывателей».

Чтобы запустить проверку конфигурации или инициализацию считывателей, необходимо в таблице установить флажки у соответствующих считывателей и выполнить соответствующую команду на панели управления (Рисунок 146).

Обобщённое состояние	Конфигуратор	Бюро пропусков	Считыватель
Elsys			
Запрос информации о считывателях завершён.			
ЛКД КЛ-60 R1 Норма	Тип считывателя: ЛКД КЛ-60 00 Режим верификации: Лицо	Количество карт: 1 Количество сигнатур: 1	Количество карт: 1 Количество сигнатур: 1
ЛКД КО-75 R2 Рассинхронизация данных	Тип считывателя: ЛКД КО-75 00 Режим верификации: Палец	Количество карт: 1 Количество сигнатур: 2	Количество карт: 1 Количество сигнатур: 3
ЛКД КО-60 R3 Рассинхронизация данных	Тип считывателя: ЛКД КО-60 00 Режим верификации: Палец	Количество карт: 1 Количество сигнатур: 2	Количество карт: 1 Количество сигнатур: 3

Рисунок 146 – Результаты проверки конфигурации биометрических считывателей

Подробный отчёт о состоянии каждого контроллера можно посмотреть в отдельном окне (Рисунок 147), выбрав пункт «Отчёт о состоянии» из контекстного меню считывателя (Рисунок 148).

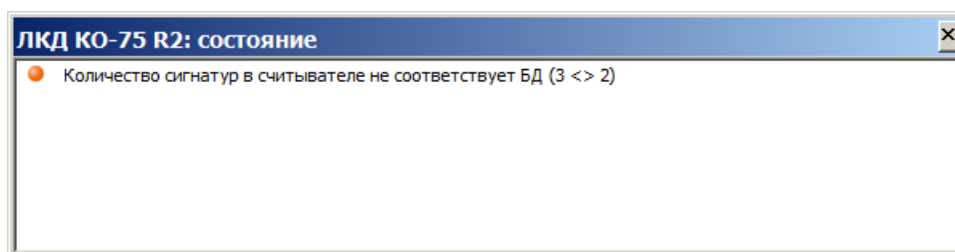


Рисунок 147 – Отчёт о состоянии считывателя

Обобщённое состояние	Конфигуратор	Бюро пропусков	Считыватель
Elsys			
Запрос информации о считывателях завершён.			
ЛКД КЛ-60 R1 Норма	Тип считывателя: ЛКД КЛ-60 00 Режим верификации: Лицо	Количество карт: 1 Количество сигнатур: 1	Количество карт: 1 Количество сигнатур: 1
ЛКД КО-75 R2 Рассинхронизация данных	Тип считывателя: ЛКД КО-75 00 Режим верификации: Палец	Количество карт: 1 Количество сигнатур: 2	Количество карт: 1 Количество сигнатур: 3
ЛКД КО-60 R3 Рассинхронизация данных	Тип считывателя: ЛКД КО-60 00 Режим верификации: Палец	Количество карт: 1 Количество сигнатур: 2	Количество карт: 1 Количество сигнатур: 3

Меню считывателя: "ЛКД КО-75 R2"

Рисунок 148 – Контекстное меню считывателя

**Внимание!** Следует учитывать, что в процессе инициализации считыватели могут работать неверно. Так, при инициализации сначала полностью очищается список карт и сигнатур в считывателе, а затем по одной заносятся новые карты и сигнатуры. Соответственно, по картам доступа и сигнатурам, которые на текущий момент времени ещё не проинициализированы, будет отказано в предоставлении доступа.



Если для профиля оператора установлено разрешение «Управление биометрическими считывателями», то в контекстном меню считывателя (Рисунок 148) доступны команды «Сброс» и «Очистить конфигурацию».

Команда «Сброс» выполняет перезапуск считывателя с сохранением всех пользовательских данных.

Команда «Очистить конфигурацию» выполняет очистку всех пользовательских данных в считывателе.

## 11 Порядок настройки СКУД Elsys для различных режимов работы

### 11.1 Общие настройки ПО «Бастион-2», используемые в работе драйвера «Бастион-2 – Elsys»

В ПО «Бастион-2» используется размер номеров карт 6 байт, для совместимости с предыдущими версиями «Бастион», а также для работы с контроллерами старых версий, в которых не поддерживаются 6-байтные номера карт, в драйвере может быть установлен размер номеров карт 3 байта. Для работы в режиме работы с 3-байтными номерами карт в драйвере реализован механизм восстановления полного 6-байтного номера по его 3-байтному значению.

Для повышения точности протоколирования событий в общих настройках ПО «Бастион-2» рекомендуется настроить синхронизацию времени, как минимум, раз в сутки (см. «Руководство системного администратора»). При этом, в заданное время будет выполняться синхронизация часов рабочих станций и подключенного к ним оборудования.

### 11.2 Настройка системы при использовании двойной идентификации (PIN-код и карта)

Если в СКУД Elsys предполагается использовать PIN-коды, необходимо выполнить ряд настроек.

В настройках контроллера Elsys-MB (п. 5.5) любых вариантов исполнения, кроме SM, следует:

- включить опцию «Использовать PIN-коды»;
- задать тип используемых клавиатур (наиболее распространены клавиатуры, совмещённые со считывателем, передающие коды клавиш по интерфейсу Wiegand);
- при необходимости изменить настройку **«Завершать ввод PIN-кода символом \*/#»**.

В настройках считывателей (п. 5.12) необходимо задать, какие устройства будут использоваться для идентификации (считыватель, клавиатура, считыватель + клавиатура). Если предполагается использование режима **«Доступ под принуждением»**, следует включить у считывателя соответствующую настройку.



В свойствах пропуска (см. инструкцию «Бюро пропусков») необходимо для каждого пользователя задать PIN-код. В драйвере Elsys допустимые значения PIN-кодов находятся в диапазоне от 1 до 65534. В бюро пропусков установлено ограничение от 1 до 9999.

### 11.3 Доступ с подтверждением картой

Доступ с подтверждением картой – встроенный усиленный алгоритм прохода, обеспечивающий для определённой категории пользователей СКУД (как правило, посетителей предприятия) доступ в отдельные точки прохода только в сопровождении лиц, уполномоченных подтверждать доступ.

На рисунке 149 показана последовательность регистрируемых событий при использовании доступа с подтверждением картой.

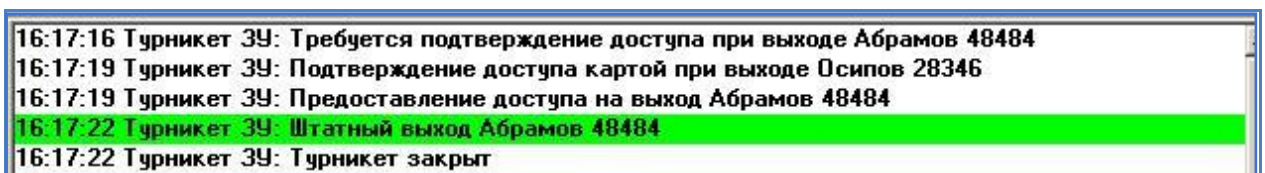


Рисунок 149– Последовательность событий при использовании режима «Доступ с подтверждением картой»

Если в течение заданного времени (задаётся настройкой **«Интервал при предъявлении нескольких карт»** на вкладке свойств считывателя **«Дополнительные»**) подтверждающая карта не будет предъявлена, будет сформировано событие «Ошибка ввода второй карты».

Для реализации режима «Доступ с подтверждением картой» необходимо настроить персональные настройки двум категориям лиц, задав им соответственно полномочия **«Доступ с подтверждением»** и **«Право подтверждать доступ»** (см. рисунки 150 - 151). Для остальных сотрудников могут быть оставлены полномочия «Обычные».

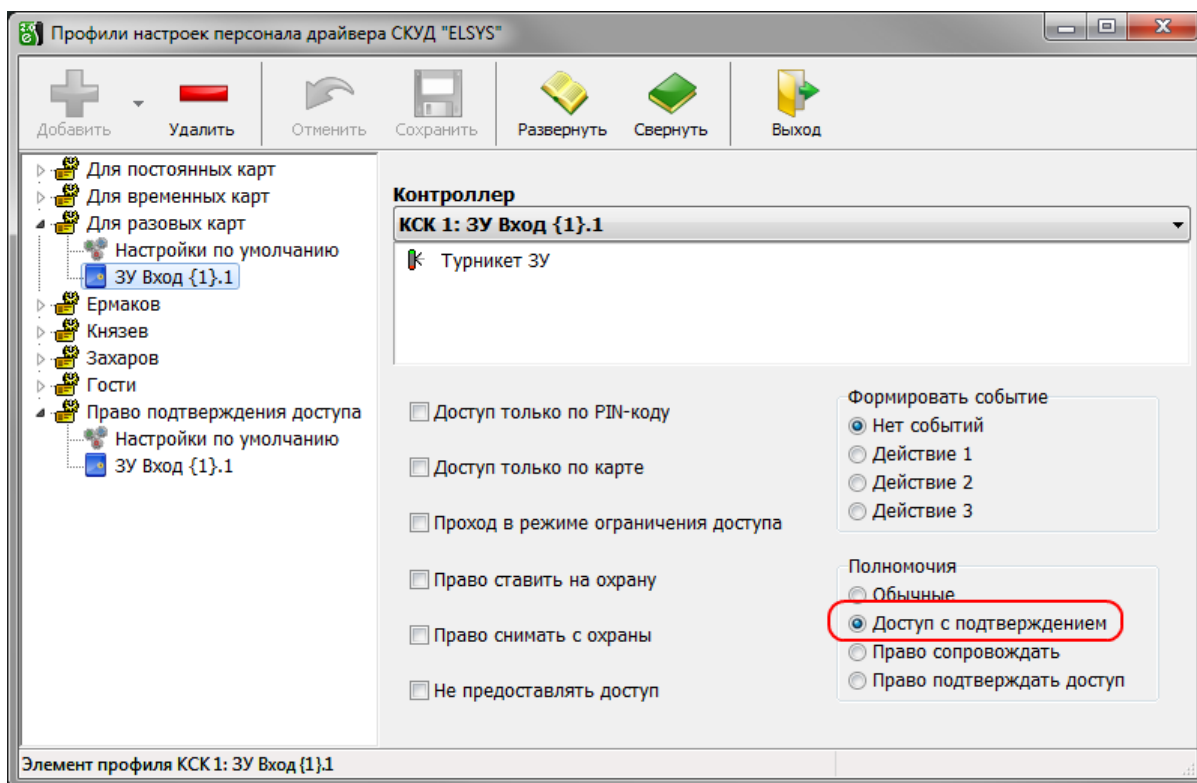


Рисунок 150 – Профиль настроек персонала для лиц, которым необходимо подтверждать доступ

Если нужно, чтобы система регистрировала также проход сотрудника, подтвердившего доступ, следует включить опцию «**Право сопровождать**» (однако, эту опцию не следует применять на турникетах, так как в этом случае одновременный проход двух сотрудников невозможен). Если нужно, чтобы подтверждающий пропуск не имел прав доступа, а использовался только для подтверждения доступа, необходимо для него включить опцию «**Не предоставлять доступ**» (обычно этот вариант используется на постах охраны).

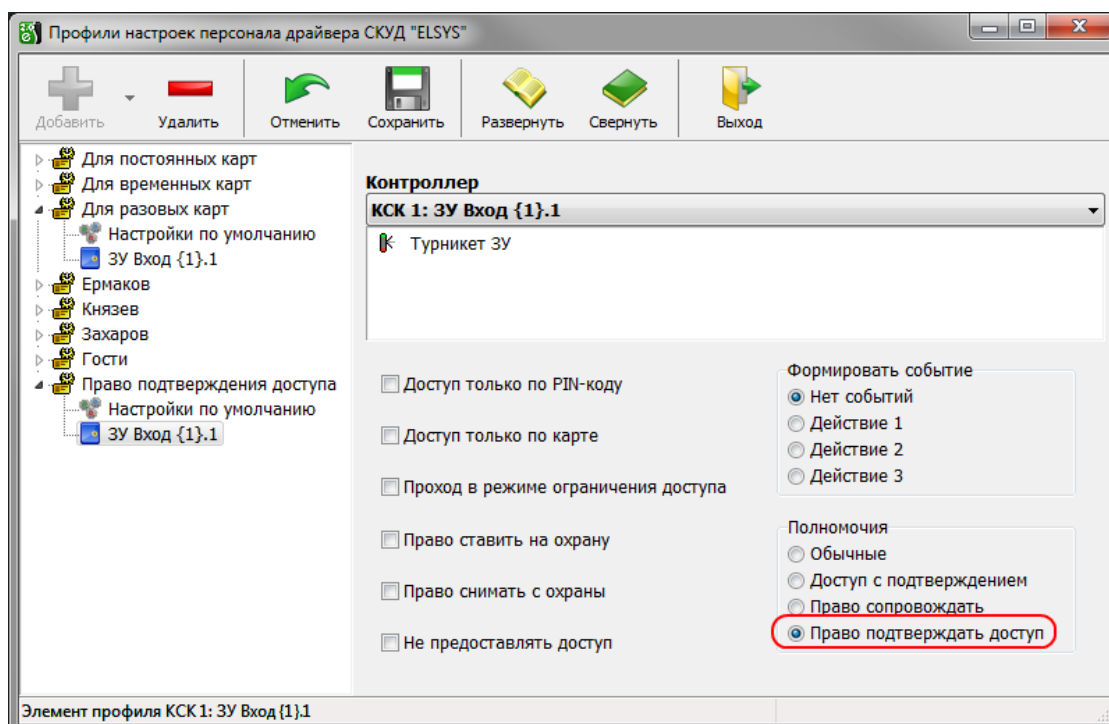


Рисунок 151 – Профиль настроек персонала для лиц, имеющих право подтверждать доступ

Для обеспечения работоспособности режима «доступ с подтверждением картой» необходимо убедиться, что на считывателе, где используется этот режим, отключены все полномочия дежурного оператора (см. рисунок 152).

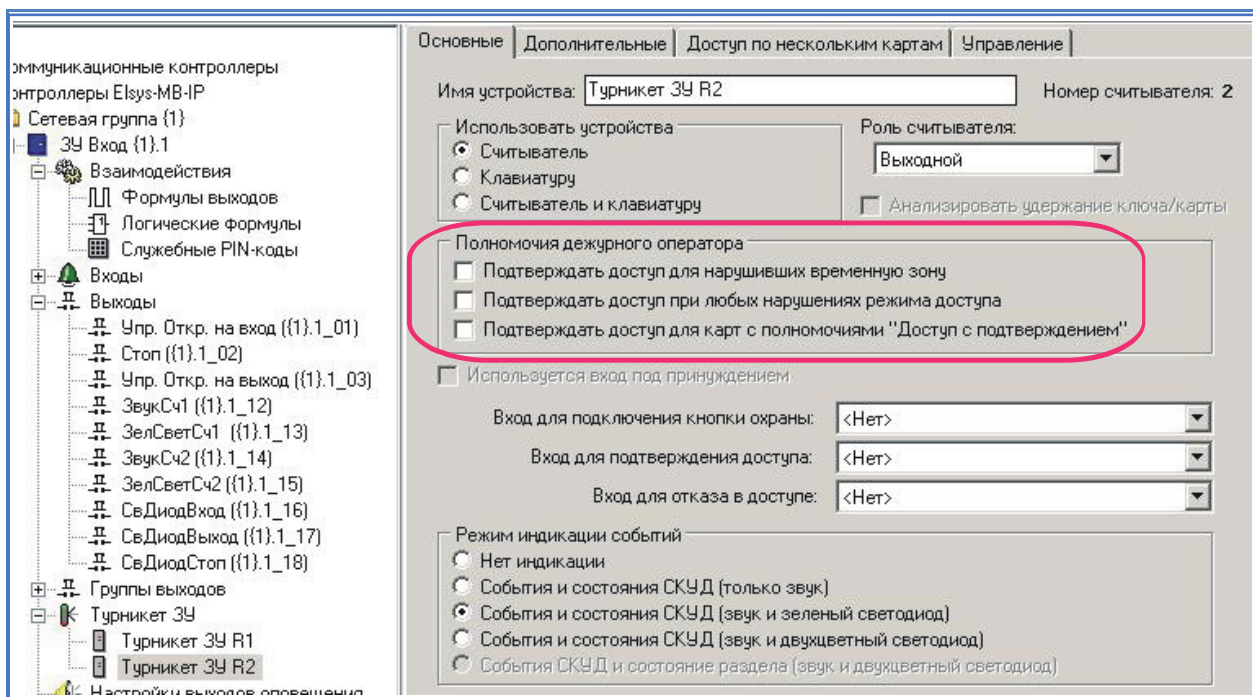
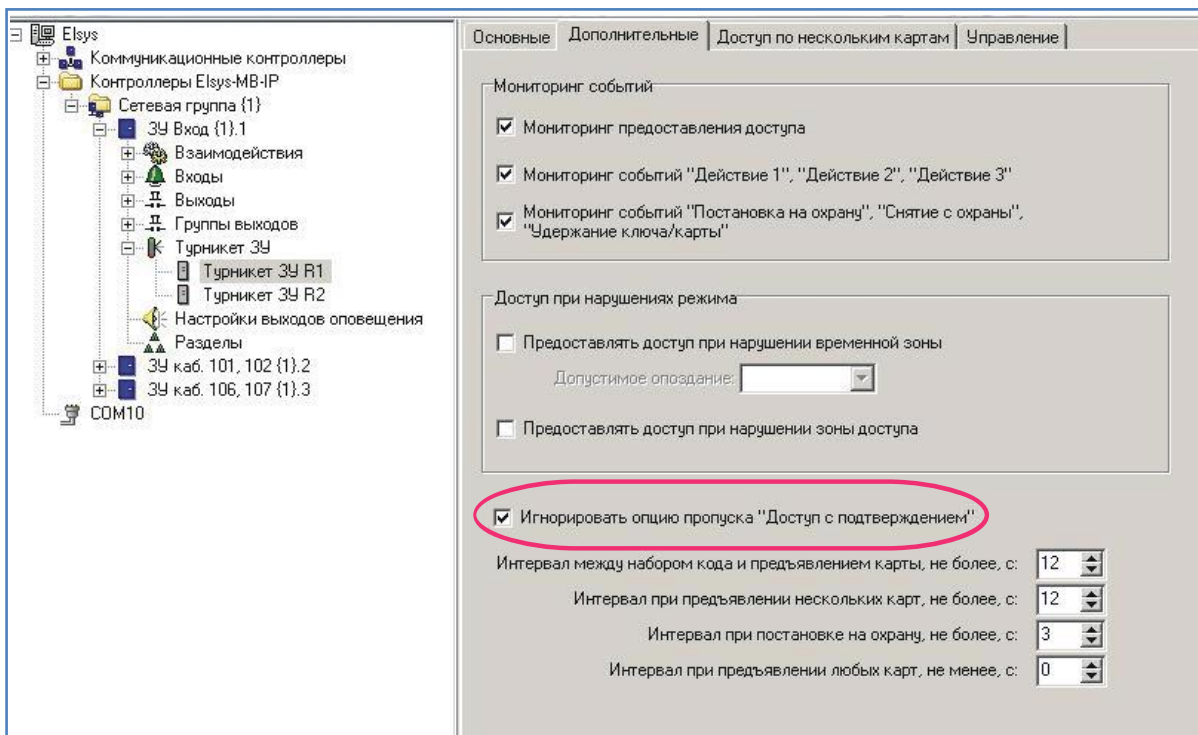


Рисунок 152 – Настройки считывателя, где используется режим «Доступ с подтверждением картой»

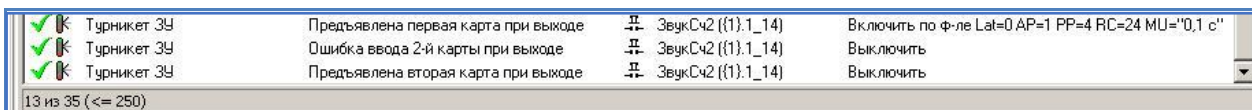
В противном случае, контроллер после предъявления карты, требующей подтверждения, будет ожидать нажатия дежурным оператором кнопки подтверждения или отказа в доступе и не будет реагировать на подтверждающую карту.

На считывателях контроллера, где режим «Доступ с подтверждением» не нужен, необходимо включить настройку **«Игнорировать опцию пропуска «Доступ с подтверждением»**» (см. рисунок 153).



**Рисунок 153 – Настройки считывателя, где необходимо выключить режимы «Доступ с подтверждением картой» и «Доступ с подтверждением кнопкой»**

После предъявления карты, требующей подтверждения, индикатор считывателя сигнализирует мигающим зелёным светодиодом о том, что необходимо подтвердить доступ. Если в дополнение к световой индикации необходимо включить звуковую индикацию, необходимо настроить взаимодействия, как показано на рисунке 154.



**Рисунок 154 – Настройка звуковой индикации ожидания подтверждающей карты**

## 11.4 Доступ с подтверждением оператором

Доступ с подтверждением оператором – встроенный усиленный алгоритм прохода, обеспечивающий для определённой категории пользователей СКУД (как правило, посетителей предприятия) доступ в отдельные точки прохода (находящиеся, как правило, на проходной предприятия) только с подтверждением дежурного оператора. На посту дежурного оператора должен быть установлен пульт с кнопками «Подтверждение доступа» и «Отказ в доступе» или "Бастион 2-АРМ оператора".

На рисунке 155 показана последовательность регистрируемых событий при использовании доступа с подтверждением кнопкой (сценарием).

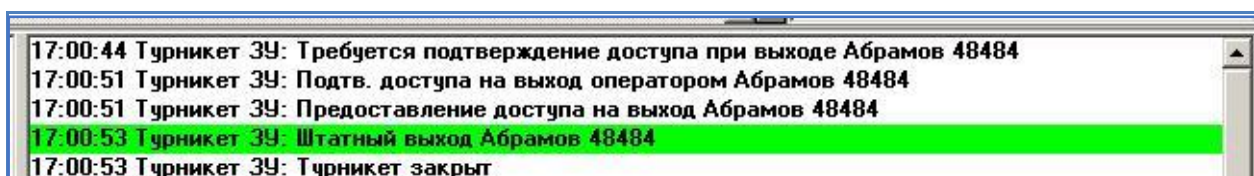


Рисунок 155– Последовательность событий при использовании режима «Доступ с подтверждением кнопкой»

Для настройки режима «Доступ с подтверждением оператором» необходимо установить персональные настройки категориям лиц, которым требуется подтверждение доступа, включив опцию **«Доступ с подтверждением»** (см. рисунок 150).

Для считывателя, где используется подтверждение доступа оператором, необходимо включить опции (см. рисунок 156):

- **«Вход для подтверждения доступа»** (вход контроллера, к которому подключена кнопка подтверждения доступа);
- **«Вход для отказа в доступе»** (вход контроллера, к которому подключена кнопка отказа в доступе);
- **«Подтверждать доступ для карт с полномочиями «Доступ с подтверждением»**.

После предъявления карты, требующей подтверждения, индикатор считывателя будет сигнализировать мигающим зелёным светодиодом о том, что необходимо подтвердить доступ. Если в дополнение к световой индикации необходимо включить звуковую индикацию, необходимо настроить взаимодействия, как показано на рисунке 157.

Оператор может подтверждать доступ, используя "Бастион 2-АРМ оператора", для чего необходимо создать соответствующий сценарий, указав в нём точку прохода и действие "Подтвердить доступ" или "Отказать в доступе". Более подробно настройка сценариев описана в документе "Бастион 2 - Руководство администратора".



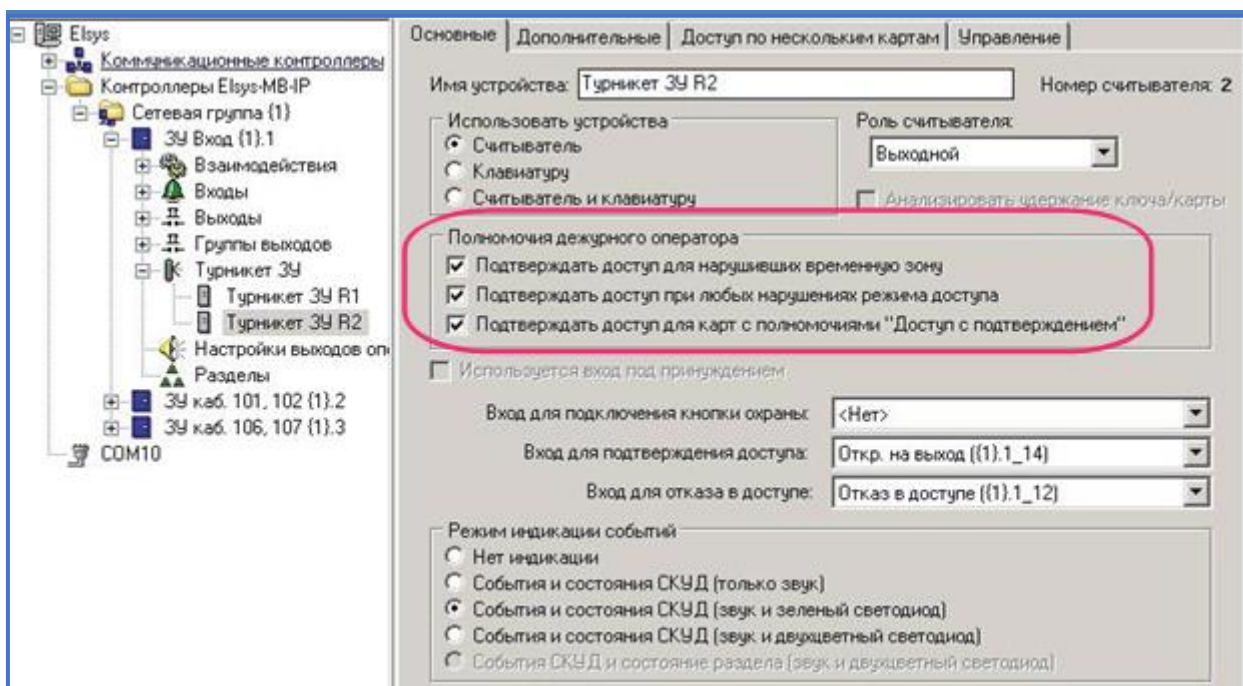


Рисунок 156– Настройки считывателя, где используется режим «Доступ с подтверждением кнопки»

✓	Турникет ЗУ	Требуется подтверждение доступа при выходе	ЗвукС42 ((1).1_14)	Включить по ф-ле Lat=0 AP=1 PP=4 RC=99 MU="0,1 с"
✓	Турникет ЗУ	Сброс режима подтверждения вых. считывателя	ЗвукС42 ((1).1_14)	Выключить
✓	Турникет ЗУ	Подтверждение доступа на выход оператором	ЗвукС42 ((1).1_14)	Выключить
✓	Турникет ЗУ	Отказ в доступе на выход оператором	ЗвукС42 ((1).1_14)	Выключить

33 из 36 (<= 250)

Рисунок 157 – Настройка звуковой индикации ожидания подтверждения оператора

## 11.5 Доступ с использованием биометрических считывателей

На рисунке 158 показана схема интеграции биометрических считывателей в составе СКУД Elsys.

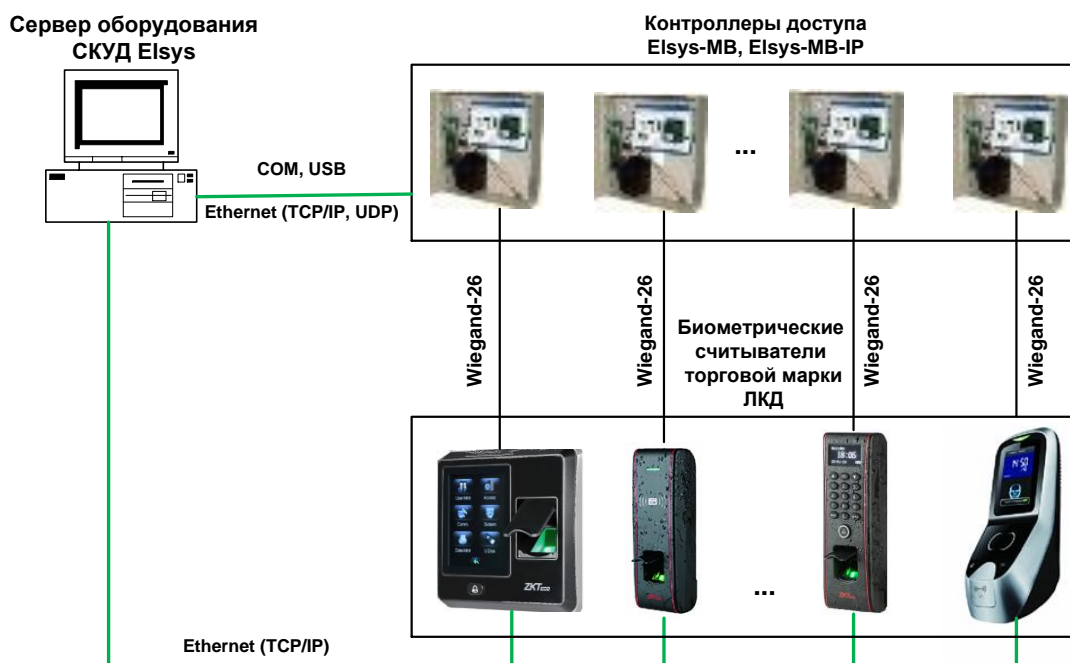


Рисунок 158 – Схема интеграции биометрии в СКУД Elsys

Биометрические считыватели должны быть подключены к контроллерам доступа Elsys по интерфейсу Wiegand, а также к серверу оборудования СКУД Elsys через Ethernet. При этом в биометрических считывателях ЛКД для выхода Wiegand должен быть установлен формат Wiegand-26. При необходимости использования считывателей EnterFace с интерфейсом, отличным от Wiegand-26, следует предварительно проконсультироваться с разработчиками Бастион-Elsys.

Подключение биометрических считывателей к контроллерам доступа Elsys через интерфейс Wiegand обеспечивает передачу кода карты пользователя при успешной идентификации, а подключение к серверу оборудования через Ethernet обеспечивает передачу в биометрические считыватели данных бюро пропусков, выполнение команд управления и запросов состояний (см. п. 10).

Настройки биометрического считывателя задаются в свойствах считывателя в конфигураторе драйвера Elsys (см.п. 5.12.4).

**Внимание!** При использовании биометрических считывателей контроллеры доступа Elsys обрабатывают сигналы от них как от считывателей без клавиатуры, поэтому все режимы прохода СКУД Elsys с использованием PIN-кодов не должны использоваться.

В дополнение к режимам прохода СКУД Elsys при использовании биометрии могут использоваться режимы верификации биометрических считывателей, приведённые в таблице 12.

## Приложения

### Приложение 1. История изменений

#### Бастион-2 – Elsys 1.2.11 (14.01.2021)

[+] Добавлена возможность настройки параметров межконтроллерного обмена в сетевой группе. Позволяет, при необходимости, ускорить межконтроллерные взаимодействия в сетевых группах с большим количеством контроллеров.

[\*] Некорректно инициализировались Elsys-IP с адресами 33-63. Исправлено.

[\*] Связь через COM-порт пропадала до перезапуска драйвера при наличии шума на линии.

[\*] Некорректно инициализировался состав раздела ОПС, при наличии в нём двери. Не работала автопостановка при выходе и тревога при взломе. Некорректно отображалось состояние раздела после снятия карты. Исправлено.

[\*] Исправлен режим опроса Elsys-IP «Через КСК по UDP», применяющийся для создания распределённых систем, в которых на каждом удалённом объекте применяется КСК и несколько контроллеров Elsys-IP, опрашиваемых через него.

*Версия «Бастион-2 – Elsys 1.2.11» протестирована с АПК «Бастион-2» версий 2.1.9 Oracle и 2.1.10 PostgreSQL.*

#### Бастион-2 – Elsys 1.2.10 (13.11.2020)

[\*] Библиотека, реализующая протокол обмена с COM-портом переписана на С# и вынесена в сборку ElsysSerial.dll.

[\*] Конфигуратор переписан на С# и вынесен в Elsys.Config.exe.

[\*] Связь через COM-порт не работала на скорости 4800. Исправлено.

[\*] При подключении Elsys-CU после старта драйвера, связь не восстанавливалась. Исправлено.

[\*] Инициализация в режиме Multimaster не начиналась при работе через COM-порт. Отмена не работала. Исправлено.

[\*] При перезапуске драйвер подвисал (остановка/запуск драйвера, сохранение конфигурации). Исправлено.

#### Бастион-2 – Elsys 1.2.9 (17.06.2020)

[\*] Для уменьшения нагрузки на сеть, отправка сетевых сообщений сетевой и серверной частями драйвера сделана адресной. Добавлен режим отправки сетевых сообщений из драйвера только известным рабочим станциям. Включается галочкой «Только известные АРМ» в дополнительных свойствах драйвера.

[+] Добавлена поддержка эмулятора MB-Net (IP-адрес MB-Net дополняется номером порта, например 192.168.21.201:4001).

[\*] Исправлена утечка памяти при ошибках связи с MB-Net.



[\*] Конфигуратор. Взаимодействие на предъявление служебной карты подсвечивается восклицательным знаком.

[\*] Конфигуратор. Отображается признак наличия ошибок в областях контроля после закрытия и открытия конфигулятора.

[\*] Не обновлялся пароль в Esys-MB-Net и Esys-IP. Исправлено.

[\*] Перезапуск и остановка драйвера выполнялись с задержкой. Исправлено.

#### **Бастион-2 – Esys 1.2.8 (20.03.2020)**

[\*] Праздники могли не попадать в драйвер и контроллеры. Исправлено.

[+] Чёрным фоном выделяются галочки в окне инициализации для контроллеров с превышением количества временных или постоянных карт, уровней доступа, временных зон, праздников.

[+] В окне инициализации теперь не отображаются исключенные из опроса контроллеры, при выключенной опции "показывать все".

[\*] В предыдущем релизе не работал адресный поиск Esys-IP. Исправлено.

[\*] Не работали сетевые группы с адресом > 1. Исправлено.

[\*] При потере и восстановлении связи с КСК и контроллерами, некорректно обновлялась доступность опций инициализации. Исправлено.

[\*] В редких случаях, после запуска / перезапуска драйвера не было событий от контроллеров, подключенных через КСК. Исправлено.

[\*] Проверка связи и конфигурации контроллеров в ряде случаев отображала неверную информацию. Исправлено.