

Группа компаний «ТвинПро»

ООО «ЕС-пром»

**ТЕХНИЧЕСКИЕ СРЕДСТВА ОХРАННОЙ СИГНАЛИЗАЦИИ  
ELSYS  
РУКОВОДСТВО ПО ЭКСПЛУАТАЦИИ**

ЕСЛА.425511.100 РЭ

## СОДЕРЖАНИЕ

1	Общие сведения.....	4
1.1	Назначение и состав ТСОС Elsys.....	4
1.2	Объекты охранной подсистемы .....	6
1.3	Функциональные возможности охранной подсистемы.....	8
1.4	Основные технические характеристики охранных контроллеров и контроллеров доступа.....	13
1.5	Основные технические характеристики клавиатуры Elsys-CP2.....	14
1.6	Технические характеристики КСК Elsys-MB-Net II и Elsys-NG-Net II ..	15
1.7	Управляющее программное обеспечение .....	16
2	Настройка локального управления охранной сигнализацией .....	18
2.1	Совместимость оборудования СКУД Elsys с локальным управлением охраной	18
2.2	Настройка охранных входов.....	18
2.3	Настройка локальных разделов.....	28
3	Настройка централизованного управления охранной сигнализацией.....	33
3.1	Совместимость оборудования СКУД Elsys с централизованным управлением охраной .....	33
3.2	Общие настройки.....	34
3.3	Настройка разделов и групп разделов.....	35
3.4	Настройка считывателей для управления режимами охраны.....	38
3.5	Настройка клавиатур Elsys-CP2 .....	39
3.6	Настройка web-клиентов для управления режимами охраны .....	42
3.7	События и состояния.....	44
3.7.1	События контроллеров .....	44
3.7.2	События охранных зон .....	44
3.7.3	События считывателей .....	45
3.7.4	События и состояния разделов .....	45
4	Управление режимами охраны .....	47
4.1	Локальное управление режимами охраны с помощью считывателей ...	47
4.1.1	Управление со считывателя охранного контроллера .....	50
4.1.2	Управление со считывателя контроллера доступа .....	50
4.2	Централизованное управление режимами охраны .....	50
4.2.1	Управление со считывателя охранного контроллера .....	50
4.2.2	Использование клавиатуры Elsys-CP2 .....	53
4.2.3	Управление через web-интерфейс браузера .....	55
4.3	Автоматизированное управление режимами охраны .....	60

4.4	Автоматическая постановка на охрану при выходе последнего сотрудника .....	61
4.5	Управление с АРМ дежурного оператора.....	65
4.6	Алгоритмы индикации считывателей .....	66
4.7	Настройка полномочий пользователей по управлению режимами охраны 70	
4.8	Программы управления выходами .....	73
4.9	Совместное использование локального и централизованного управления 78	
5	Дополнительные сведения по настройке охранной подсистемы.....	79
5.1	Начальная настройка КСК и охранных контроллеров .....	79
5.2	Начальная настройка устройств адресной двухпроводной линии .....	81
5.3	Загрузка конфигурации системы в оборудование (инициализация оборудования) .....	83
5.3.1	Инициализация аппаратных настроек.....	83
5.3.2	Инициализация настроек персонала .....	84

Настоящее руководство по эксплуатации предназначено для изучения принципа работы, настройки и эксплуатации технических средств охранной сигнализации (далее – ТСОС) Elsys.

В настоящем руководстве приняты следующие сокращения и обозначения:

ОС – охранная сигнализация;

ТСОС – технические средства охранной сигнализации;

СКУД – система контроля и управления доступом;

ПО – программное обеспечение;

ПК – персональный компьютер;

ППКО – прибор приёмно-контроллер охранный;

ШС – шлейф сигнализации;

PIN-код – дополнительный идентификационный признак, вводимый с клавиатуры;

КСК – коммуникационный сетевой контроллер;

АДЛС – адресная двухпроводная линия связи;

ГУО – группа управления охраной.

Версия настоящего документа – 1.06 (10.2024).

## **1 Общие сведения**

### **1.1 Назначение и состав ТСОС Elsys**

Система охранной сигнализации, построенная на основе технических средств охранной сигнализации Elsys, предназначена для защиты объектов от несанкционированных проникновений путём регистрации, обработки, передачи и отображения информации о состоянии шлейфов охранной сигнализации.

Технические средства охранной сигнализации Elsys, обеспечивающие работу охранной подсистемы СКУД Elsys, могут использоваться как самостоятельно, так и совместно с техническими средствами контроля и управления доступом Elsys.

ТСОС Elsys обеспечивают:

- контроль состояния шлейфов сигнализации (далее – ШС);
- антисаботажную защиту ШС путём подключения оконечного резистора;
- объединение ШС в разделы для группового управления охраной;
- передачу тревожных извещений в управляющее программное обеспечение;
- выдачу тревожных извещений на пульт централизованного наблюдения (ПЦН) через релейные выходы устройств охранной подсистемы;
- управление звуковыми и световыми индикаторами и оповещателями по заданным программам;
- ведение базы данных идентификационных признаков сотрудников с назначенными полномочиями по управлению режимами охраны;
- авторизованное управление режимами охраны с использованием бесконтактных карт доступа и/или пользовательских паролей (PIN-кодов);
- централизованное управление охраной по командам, передаваемым от автоматизированных рабочих мест оператора;
- работу всех основных функций в случае нарушения связи с управляющим программным обеспечением.

В состав охранной подсистемы СКУД Elsys входят следующие ТСОС:

- коммуникационные сетевые контроллеры Elsys-MB-Net II и Elsys-NG-Net II;
- охранные контроллеры Elsys-MB-AC и Elsys-AC2;
- расширители шлейфов сигнализации Elsys-AC-AE2, Elsys-AC-AE8, подключаемые в АДЛС охранного контроллера Elsys-AC2;
- релейные модули Elsys-AC-RM2, подключаемые в АДЛС охранного контроллера Elsys-AC2;
- адресные извещатели Elsys-AC-IRV, Elsys-AC-GB, Elsys-AC-IRF, Elsys-AC-MS, подключаемые в АДЛС охранного контроллера Elsys-AC2;
- клавиатура Elsys-CP2, обеспечивающая во взаимодействии с КСК Elsys-MB-Net II или Elsys-NG-Net II оперативное управление и отображение состояния охранных разделов.

Кроме того, в составе охранной подсистемы могут использоваться контроллеры доступа с функциями охранной сигнализации:

- Elsys-MB вариантов исполнения Pro, Std, Light, Pro4;
- Elsys-NG-200, Elsys-NG-800 и Elsys-NG-1000 (далее – Elsys-NG-xx).

Оборудование СКУД Elsys обеспечивает аппаратную интеграцию подсистем контроля и управления доступом и охранной сигнализации и подключается к серверу интеграции по общим каналам связи одним из трёх способов:

- по двухпроводному интерфейсу RS-485 через преобразователь интерфейсов (Elsys-RC-232/485, Elsys-CU-USB/232-485);
- по двухпроводному интерфейсу RS-485 через коммуникационный сетевой контроллер Elsys-MB-Net, Elsys-MB-Net II или Elsys-NG-Net II;
- по интерфейсу Ethernet (в этом случае обмен данными с контроллером может выполнять либо сервер интеграции, либо КСК).

Коммуникационные сетевые контроллеры Elsys-MB-Net II и Elsys-NG-Net II, кроме базовых функций КСК, могут выполнять функции центрального контроллера охранной сигнализации в составе прибора приёмно-контрольного охранного блочно-модульного Elsys.

Прибор приёмно-контрольный охранный блочно-модульный Elsys ЕСЛА.425511.100-01 (далее – ППКО Elsys) – совокупность аппаратных средств, обеспечивающих работу сегмента централизованной охранной сигнализации под управлением КСК. В состав ППКО Elsys входит один КСК Elsys-MB-Net II или КСК Elsys-NG-Net II и оборудование ТСОС, в количестве, определяемом потребностями заказчика и не превышающем заявленные в таблице (Таблица 3) адресную ёмкость и количественные характеристики прибора.

## 1.2 Объекты охранной подсистемы

В настоящем разделе дано определение и описание основных объектов охранной подсистемы.

*Охранный контроллер* – устройство, обеспечивающее сбор и первичную обработку информации от датчиков охранной сигнализации, и локальное управление охранной сигнализацией. Кроме специализированных охранных контроллеров Elsys-MB-AC и Elsys-AC2, функции охранного контроллера могут

выполнять также контроллеры доступа Elsys-MB вариантов исполнения Light, Std, Pro, Pro4 и контроллеры доступа Elsys-NG-xx.

*Центральный контроллер охранной сигнализации (ЦКОС)* – устройство, выполняющее сбор и обработку информации от охранных контроллеров, и обеспечивающее централизованное управление охранной сигнализацией. Функции ЦКОС в СКУД Elsys выполняет коммуникационный сетевой контроллер Elsys-MB-Net II или Elsys-NG-Net II.

*Блок управления и индикации* – устройство, предназначенное для оперативного управления и отображения состояния охранных разделов. В СКУД Elsys функции блока управления и индикации выполняет клавиатура Elsys-CP2, работающая в составе централизованной системы охраны, работающей под управлением КСК Elsys-MB-Net II или Elsys-NG-Net II.

*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 нормально замкнутые или нормально разомкнутые контакты.

*Охранный раздел* – логическое объединение нескольких охранных зон для группового управления, взаимодействия и мониторинга. Раздел, управление которым осуществляет охранный контроллер, называется локальным. Раздел, управление которым осуществляет КСК Elsys-MB-Net II или Elsys-NG-Net II, называется глобальным. В состав локального раздела могут входить зоны одного охранного контроллера, а в состав глобального раздела могут входить зоны нескольких охранных контроллеров. Зона может входить в состав только одного раздела.

*Группа разделов* – логическое объединение нескольких разделов для совместного управления, взаимодействия и мониторинга под управлением КСК Elsys-MB-Net II или Elsys-NG-Net II. Группа разделов обладает всеми свойствами раздела и имеет тот же набор команд, событий и полномочий для управления охраной. Любой раздел может входить в несколько групп разделов.

*Выходы оповещения* – физические выходы охранных контроллеров или контроллеров доступа (как правило, релейные) для которых назначен список объектов охранной сигнализации (охранных зон или разделов), на события которых этот выход должен реагировать по заданной программе управления («ПЦН», «Лампа» и т. д.). Если выход используется в качестве выхода оповещения охранной сигнализации, для него недоступно непосредственное управление.

*Точки управления охраной* – устройства, с которых может выполняться управление режимами охранной сигнализации. Кроме блоков управления и индикации, точками управления охраной могут быть считыватели, подключенные к охранным контроллерам или контроллерам доступа.

*Пользователь охранной сигнализации* – сотрудник, имеющий необходимые полномочия для постановки помещений на охрану и/или снятия их с охраны.

*Группа управления охраной* – заранее настроенный набор полномочий, назначаемый пользователям охранной сигнализации. Этот набор является списком разделов охранной системы с назначенными для каждого из них полномочиями по управлению охраной.

*Локальное управление охранной сигнализацией* – управление режимами охраны локальных разделов и устройствами оповещения средствами охранного контроллера.

*Централизованное управление охранной сигнализацией* – управление режимами охраны глобальных разделов и устройствами оповещения средствами КСК.

### 1.3 Функциональные возможности охранной подсистемы

Структурная схема охранной подсистемы изображена на рисунке (Рисунок 1).

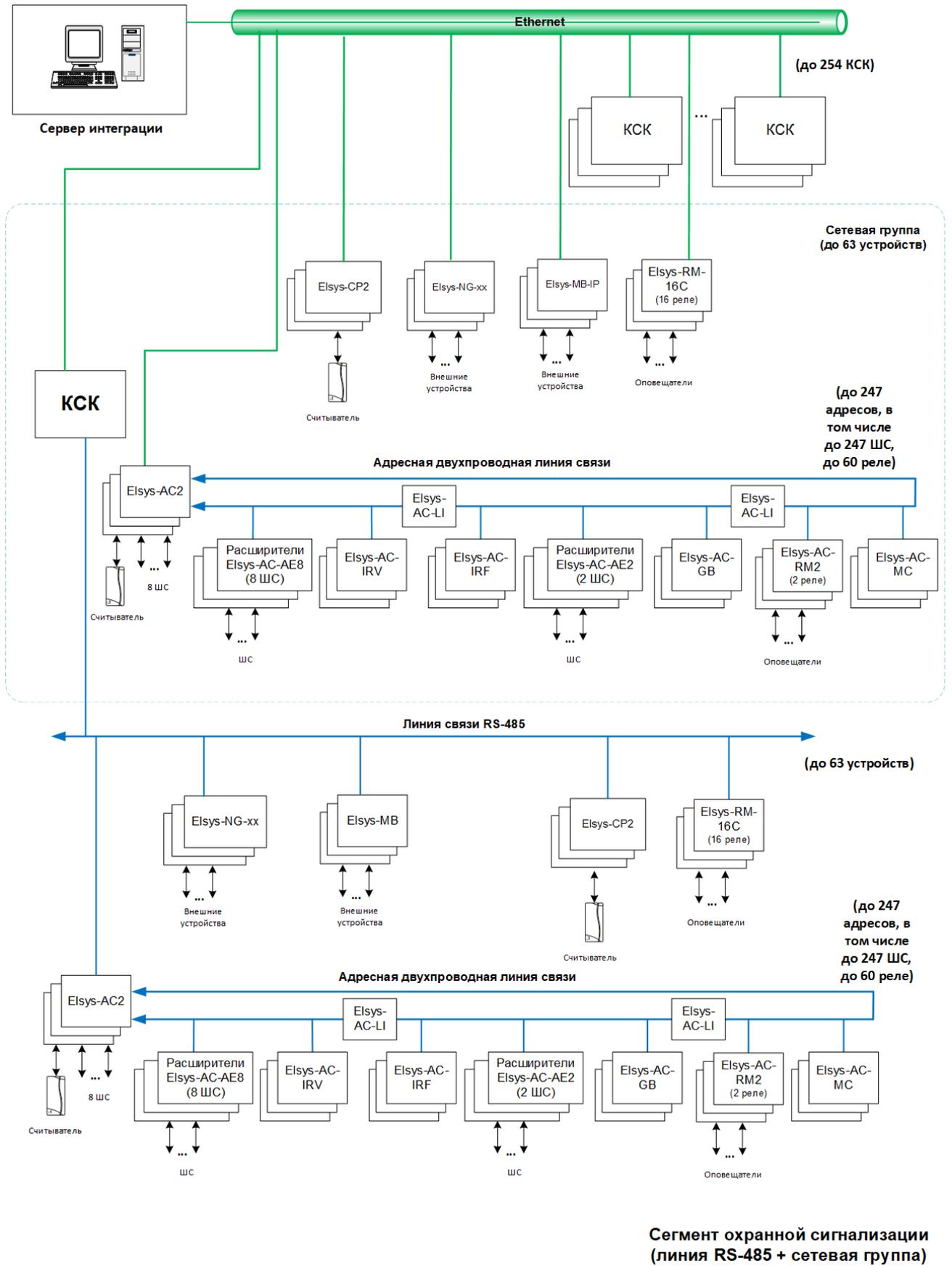


Рисунок 1. Структурная схема охранной подсистемы

В охранной подсистеме могут использоваться два режима управления – локальный и централизованный.

В локальном режиме охранные контроллеры или контроллеры доступа полностью обеспечивают логику работы сегментов охранной сигнализации, состоящих из устройств, подключенных к ним.

В этом режиме контроллеры обеспечивают:

- контроль состояния встроенных ШС и ШС устройств АДЛС;
- управление встроенными релейными выходами и выходами устройств АДЛС;
- антисаботажную защиту встроенных ШС путём подключения оконечного резистора;
- объединение встроенных ШС и ШС устройств АДЛС в разделы для группового управления охраной;
- индикацию состояний разделов звуковым и светодиодным индикаторами считывателя;
- передачу тревожных извещений в КСК или на сервер интеграции по интерфейсам RS-485 и Ethernet;
- выдачу тревожных извещений на пульт централизованного наблюдения (ПЦН) через собственные релейные выходы и выходы устройств АДЛС;
- управление внешними звуковыми и световыми индикаторами и оповещателями по заданным программам;
- автоматизированное локальное управление охраной с использованием бесконтактных карт доступа или электронных ключей Touch Memory;
- возможность использования встроенной в считыватель клавиатуры для ввода параметров управления охранными разделами;
- управление охраной по командам, передаваемым от КСК или сервера интеграции;
- настройку и хранение в энергонезависимой памяти параметров ШС, разделов, релейных выходов, входов и выходов устройств АДЛС;

- настройку и хранение в энергонезависимой памяти базы данных идентификационных признаков сотрудников с назначенными полномочиями по управлению режимами охраны;
- регистрацию и накопление событий (с ведением даты и времени) в энергонезависимой памяти контроллера. При установлении связи все события, накопленные в памяти контроллера, передаются в КСК или на сервер интеграции;
- работу всех основных функций в автономном режиме и при нарушении связи с КСК или сервером интеграции.

При использовании централизованного управления охранной сигнализацией КСК Elsys-MB-Net II или Elsys-NG-Net II, выполняющий функции центрального контроллера охранной сигнализации (далее – ЦКОС), обеспечивает управление сегментом охранной сигнализации, состоящего из устройств, подключенных к линиям связи КСК (до 63 устройств в линии связи RS-485 и до 63 устройств в сетевой группе).

В энергонезависимой памяти КСК содержится конфигурация охранной подсистемы:

- список и состав глобальных разделов и групп разделов;
- список считывателей, участвующих в централизованном управлении охраной, и их настройки;
- настройки выходов оповещения;
- списки разделов, назначенных для передачи на устройства управления и индикации.

Перечисленные выше настройки редактируются в конфигураторе оборудования и затем при инициализации оборудования целиком загружаются в КСК.

Кроме того, в энергонезависимой памяти КСК содержится список пользователей охранной сигнализации и состав групп управления охраной, назначаемых им. Эти данные могут быть оперативно загружены из клиентского программного обеспечения. КСК обеспечивает также автоматическую синхронизацию базы данных пользователей и их полномочий, что позволяет всегда поддерживать их в актуальном состоянии.

В централизованном режиме управления охранной сигнализацией КСК обеспечивает:

- сбор и протоколирование событий от охранных контроллеров и контроллеров доступа, обслуживающих входы, включённые в глобальные разделы и локальные разделы, включённые в список для глобального управления;
- формирование логических состояний глобальных разделов на основе анализа текущих состояний охранных зон, входящих в их состав;
- формирование логических состояний групп разделов на основе анализа текущих состояний разделов, входящих в их состав;
- регистрацию событий, отображающих действия пользователей по управлению режимами охраны и изменение логических состояний глобальных разделов и групп разделов;
- формирование логических состояний для выходов оповещения на основе интегрированного состояния разделов, связанных с ними;
- автоматическое формирование команд по управлению выходами оповещения;
- формирование команд для контроллеров, обеспечивающих управление режимами охраны глобальных разделов по внешним командам или по командам, принятым из точек управления охраной;
- автоматическую передачу состояний охранных разделов на блоки управления и индикации;
- приём и анализ запросов на управление охраной, поступающих с блоков управления и индикации и со считывателей охранных контроллеров;
- анализ полномочий пользователей, выполняющих централизованное управление охраной;
- ведение протокола событий охранной подсистемы и передачу накопленных событий в клиентское программное обеспечение.

В централизованном режиме управления охраной охранные контроллеры Elsys-MB-AC и Elsys-AC2, контроллеры доступа Elsys-MB и контроллеры доступа Elsys-NG-xx выполняют первичную обработку информации о состоянии

охранных зон и локальных разделов и передают состояния и события от этих устройств в КСК.

#### 1.4 Основные технические характеристики охранных контроллеров и контроллеров доступа

В таблице (Таблица 1) приведены основные технические характеристики охранных контроллеров и контроллеров доступа, актуальные при использовании их в охранной подсистеме.

Таблица 1.  
Основные технические характеристики охранных контроллеров и контроллеров доступа

Наименование параметра	Тип контроллера								
	Elsys-MB-AC	Elsys-AC2	Elsys-MB				Elsys-NG-200	Elsys-NG-800	Elsys-NG-1000
			Pro	Std	Light	Pro4			
Количество встроенных входов для подключения шлейфов сигнализации	8	8	8	4	8	8	8	8	8
Количество встроенных релейных выходов	2	4	4	3	4	4	3	4	4
Количество считывателей <sup>1)</sup>	1	1	2	2	4	4	2	4	4
Количество входов АДЛС	–	247	–				–	–	–
Количество выходов АДЛС	–	60	–				–	–	–
Адресная ёмкость АДЛС	–	247	–				–	–	–
Количество локальных охранных разделов	8	255	8	4	8	8	8	8	8
Количество пользователей <sup>2)</sup>	1024	64000	160000				75000	400000	400000
Максимальное количество событий в энергонезависимой памяти	2048	16000	120000				250000	500000	700000
Количество групп управления охраной <sup>2)</sup>	1024	64000	–				–	–	–

Наименование параметра	Тип контроллера								
	Elsys-MB-AC	Elsys-AC2	Elsys-MB				Elsys-NG-200	Elsys-NG-800	Elsys-NG-1000
			Pro	Std	Light	Pro4			
Интерфейс линии связи с КСК или сервером интеграции	RS-485	RS-485 Ethernet	RS-485 Ethernet <sup>3)</sup>				RS-485 Ethernet	RS-485 Ethernet	RS-485 Ethernet
Адресная двухпроводная линия связи	–	+	–				–	–	–
Диапазон допустимых напряжений на входах, В	0 – 5	0 – 11,5	0 – 13,2				0 – 12	0 – 12	0 – 12
Номинальное значение оконечного резистора для охранного ШС, кОм	2	2	2				2	2	2
Номинальное значение оконечного резистора для ШС устройств АДЛС, кОм	–	10	–				–	–	–
Примечания: 1 Считыватели в контроллерах доступа Elsys-MB и Elsys-NG-xx могут использоваться только для локального управления охраной и не могут участвовать в централизованном управлении охраной. 2 В контроллерах Elsys-MB и Elsys-NG-xx не разграничиваются полномочия пользователей по управлению разными локальными разделами. Все пользователи СКУД, имеющие полномочия «Право постановки на охрану» и/или «Право снятия с охраны» имеют соответствующие полномочия по управлению любыми локальными разделами контроллера. 3 При наличии модуля Ethernet-интерфейса Elsys-IP.									

Полностью технические характеристики перечисленных выше изделий приведены в соответствующих руководствах по эксплуатации.

### 1.5 Основные технические характеристики клавиатуры Elsys-CP2

Основные технические характеристики клавиатуры Elsys-CP2, актуальные при использовании её в централизованной охранной подсистеме, приведены в таблице (Таблица 2).

Таблица 2.  
Основные технические характеристики клавиатуры Elsys-CP2

Наименование параметра	Значение
Интерфейс линии связи с КСК	Ethernet, двухпроводный RS-485

Наименование параметра	Значение
Количество отображаемых на экране разделов в режиме «Индикация и управление»	40
Встроенный звуковой индикатор	Есть
Количество подключаемых считывателей	1
Режимы управления и индикации	<ul style="list-style-type: none"> <li>• «Клавиатура»</li> <li>• «Индикация и управление»</li> </ul>
Способ идентификации пользователей	<ul style="list-style-type: none"> <li>• «Карта»</li> <li>• «PIN-код»</li> <li>• «Карта и PIN-код»</li> <li>• «Карта или PIN-код»</li> </ul>

Клавиатура предназначена для централизованного управления охранной сигнализацией при совместной работе с КСК Elsys-MB-Net II или Elsys-NG-Net II.

Подробное описание клавиатуры приведено в документе «Elsys-CP2. Руководство по эксплуатации».

#### 1.6 Технические характеристики КСК Elsys-MB-Net II и Elsys-NG-Net II

В таблице (Таблица 3) приведены основные характеристики КСК Elsys-MB-Net II и Elsys-NG-Net II, актуальные при их использовании в централизованной охранной подсистеме в составе ППКО Elsys.

Таблица 3.  
Технические характеристики ЦКОС

Наименование параметра	Значение
Интерфейс связи с сервером интеграции	Ethernet
Интерфейс связи с оборудованием СКУД и охранной сигнализации	RS-485, Ethernet
Максимальное количество контроллеров в линии RS-485	63
Максимальное количество контроллеров сетевой группы, подключаемых по интерфейсу Ethernet	63
Количество охранных зон, обслуживаемых одним КСК	4096
Количество разделов	4096
Количество групп разделов <sup>1)</sup>	2048

Наименование параметра	Значение
Количество программируемых выходов	512
Количество пользователей охранной сигнализации	64000
Количество групп управления охраной <sup>2)</sup>	64000
Примечания: 1 В КСК нет никаких дополнительных ограничений на количественный состав групп разделов. Однако, следует учитывать, что при очень большом количестве групп разделов и большом количестве разделов в группах быстродействие системы может снизиться. 2 Количество групп управления охраной приведено при условии, что среднее количество разделов в группе не превышает пяти. Соответственно, если среднее число разделов в группе равно 500, то в память КСК может быть занесено до 640 групп управления охраной.	

### 1.7 Управляющее программное обеспечение

**ВНИМАНИЕ!** Перед началом настройки охранной подсистемы СКУД Elsys необходимо ознакомиться с документом «СКУД Elsys. Руководство по настройке» и руководствами по эксплуатации сервера интеграции, конфигуратора оборудования СКУД Elsys и клиентского программного обеспечения.

Функциональная схема, описывающая взаимодействие программных и аппаратных средств СКУД Elsys, приведена на рисунке (Рисунок 2).

Управляющее программное обеспечение является клиентским приложением сервера интеграции, в состав которого могут входить различные программные модули, выпускаемые группой компаний «ТвинПро» или её партнёрами. Номенклатура и количество программных модулей, входящих в состав клиентского программного обеспечения (сервер системы, серверы оборудования, АРМ дежурного оператора, АРМ оператора бюро пропусков, генераторы отчётов и т. п.) определяется спецификой объекта и потребностями заказчика.

Сервер интеграции, реализованный в виде программного сервиса, обеспечивает информационный обмен клиентского программного обеспечения с оборудованием СКУД Elsys. Сервер интеграции может быть развёрнут как на

выделенном компьютере (сервере оборудования), так и на том же компьютере, где установлено клиентское программное обеспечение.

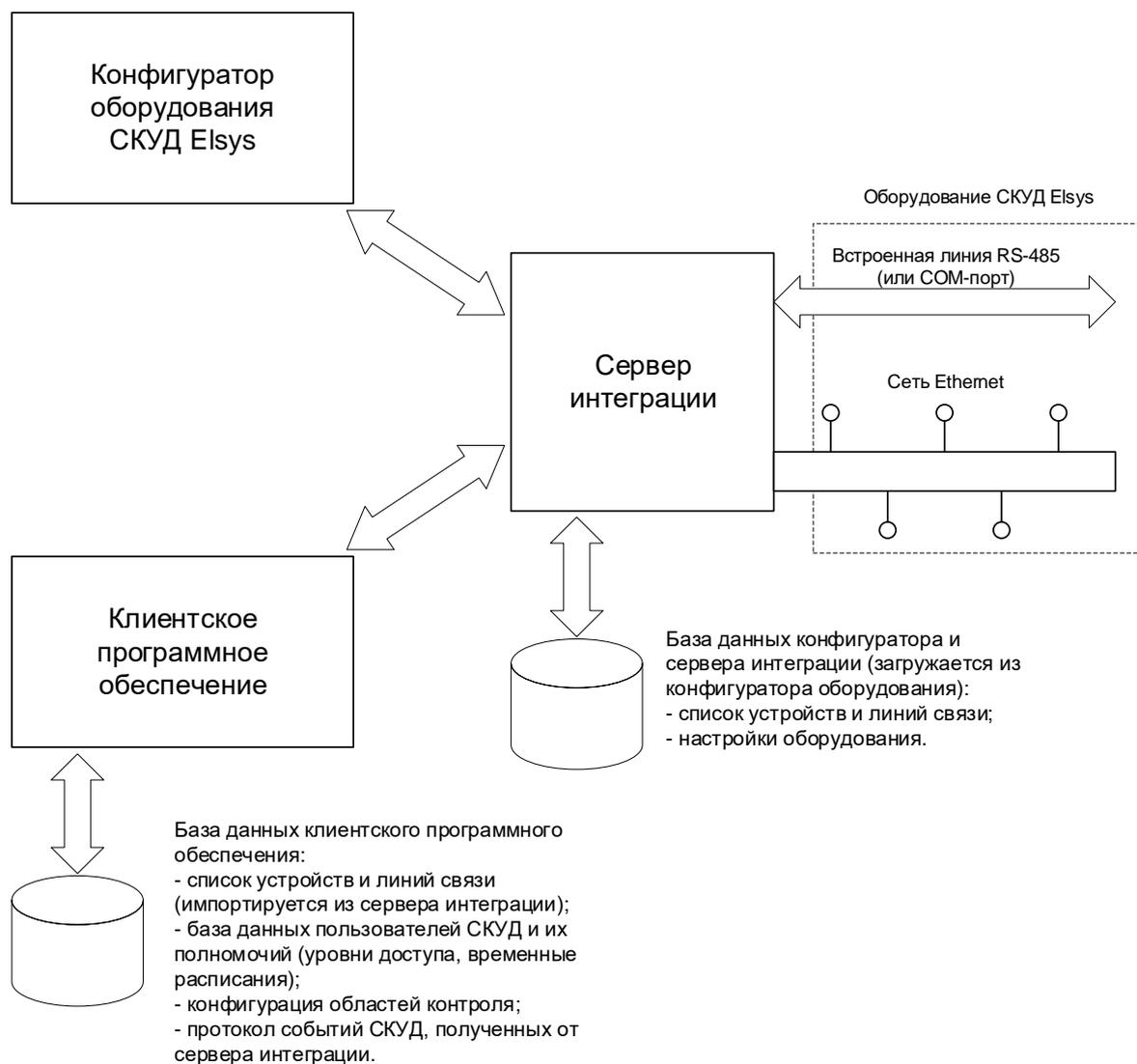


Рисунок 2. Взаимодействие программных и аппаратных средств

Конфигуратор СКУД Elsys выполняет настройку и загрузку в оборудование параметров системы, обновление встроенного программного обеспечения (прошивок) оборудования, и прочие сервисные функции.

## 2 Настройка локального управления охранной сигнализацией

### 2.1 Совместимость оборудования СКУД Elsys с локальным управлением охраной

Локальное управление охраной могут осуществлять:

- охранные контроллеры Elsys-MB-AC версий не ниже 2.02;
- охранные контроллеры Elsys-AC2;
- контроллеры доступа Elsys-MB, оснащённые модулем расширения памяти и имеющие версию встроенного программного обеспечения не ниже 2.60;
- контроллеры доступа Elsys-NG-xx.

Контроллеры, использующие локальное управление охраной, могут быть подключены к серверу интеграции как непосредственно, так и через КСК Elsys-MB-Net, Elsys-MB-Net II или Elsys-NG-Net II.

**ВНИМАНИЕ! Совместная работа КСК Elsys-MB-Net и охранных контроллеров Elsys-AC2 не поддерживается, поэтому контроллеры Elsys-AC2 следует подключать к серверу интеграции через КСК Elsys-MB-Net II, Elsys-NG-Net II или непосредственно (по RS-485 или Ethernet).**

### 2.2 Настройка охранных входов

Встроенные входы контроллера и входы адресных устройств АДЛС предназначены для подключения шлейфов сигнализации. ШС представляет собой электрическую цепь, в которую объединены охранные извещатели, подключенные к одному охранному входу контроллера или устройства АДЛС и обеспечивающие обслуживание одной охранной зоны.

ШС, относящиеся к одному контроллеру (как встроенные, так и обслуживаемые устройствами АДЛС), могут быть сгруппированы в локальные разделы. Любые ШС могут входить не более чем в один раздел.

Настройка входов контроллера заключается в задании параметров добавленным входам в окне конфигуратора. Окно настройки входа приведено на рисунке (Рисунок 3).

Встроенные входы контроллеров могут использоваться в качестве входов общего назначения. В этом режиме для них недоступно участие в разделах,

однако доступен ряд дополнительных функциональных возможностей (см. Рисунок 4).

В окне настройки входа в выпадающем списке «Номер входа» можно выбрать конкретный вход, нумерация которого соответствует его физическому расположению на плате применяемого контроллера. Вход может быть как аналоговым, так и цифровым (о типе входов используемого контроллера написано в руководстве по эксплуатации на этот контроллер).

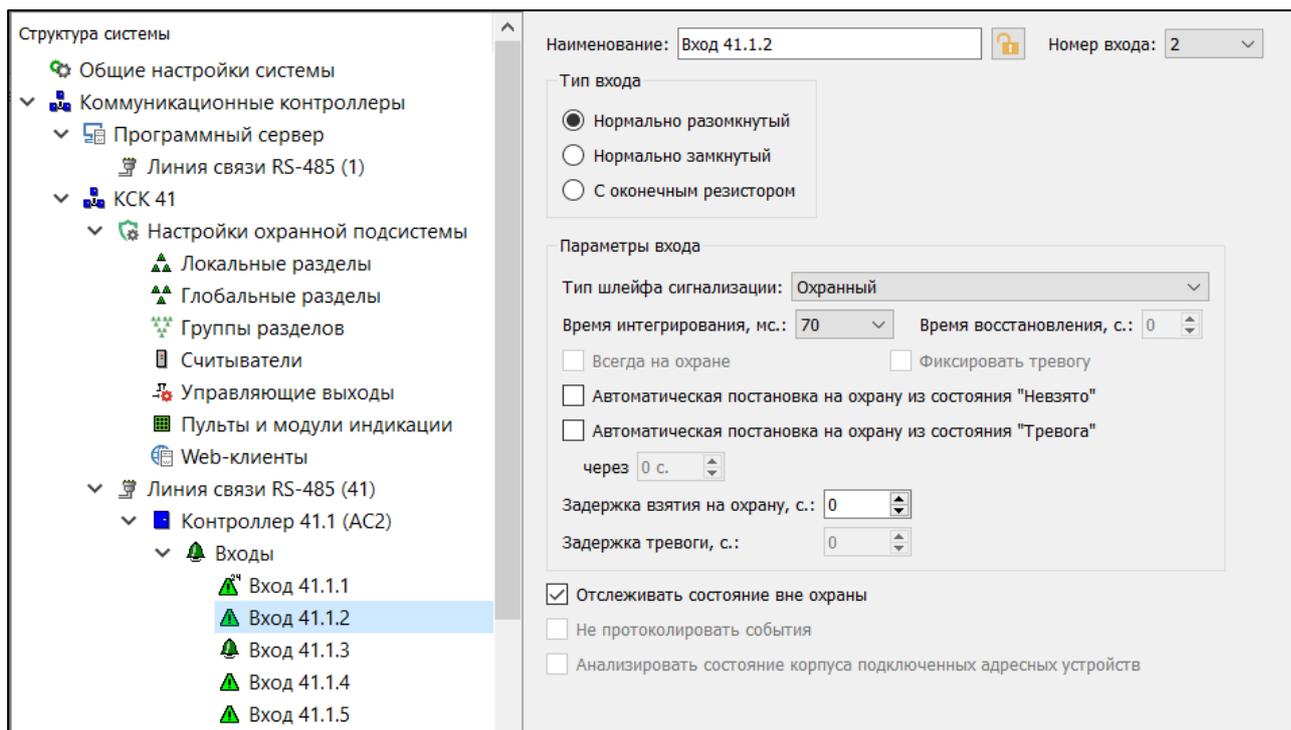


Рисунок 3. Окно настройки входа

Тип входа – настройка, позволяющая выбрать тип подключения, который будет использоваться в конфигурации, при этом только для аналоговых входов доступна возможность выбрать оконечный резистор.

Всего возможно восемь комбинаций параметров для описания типа входа:

- Нормально разомкнутый;
- Нормально замкнутый;
- Нормально замкнутый с оконечным резистором;
- Нормально разомкнутый с оконечным резистором;
- Оба типа датчиков с оконечным резистором;

- Нормально разомкнутый с оконечным резистором и добавочными резисторами;
- Нормально замкнутый с оконечным резистором и добавочными резисторами;
- Оба типа датчиков с оконечным резистором и добавочными резисторами.

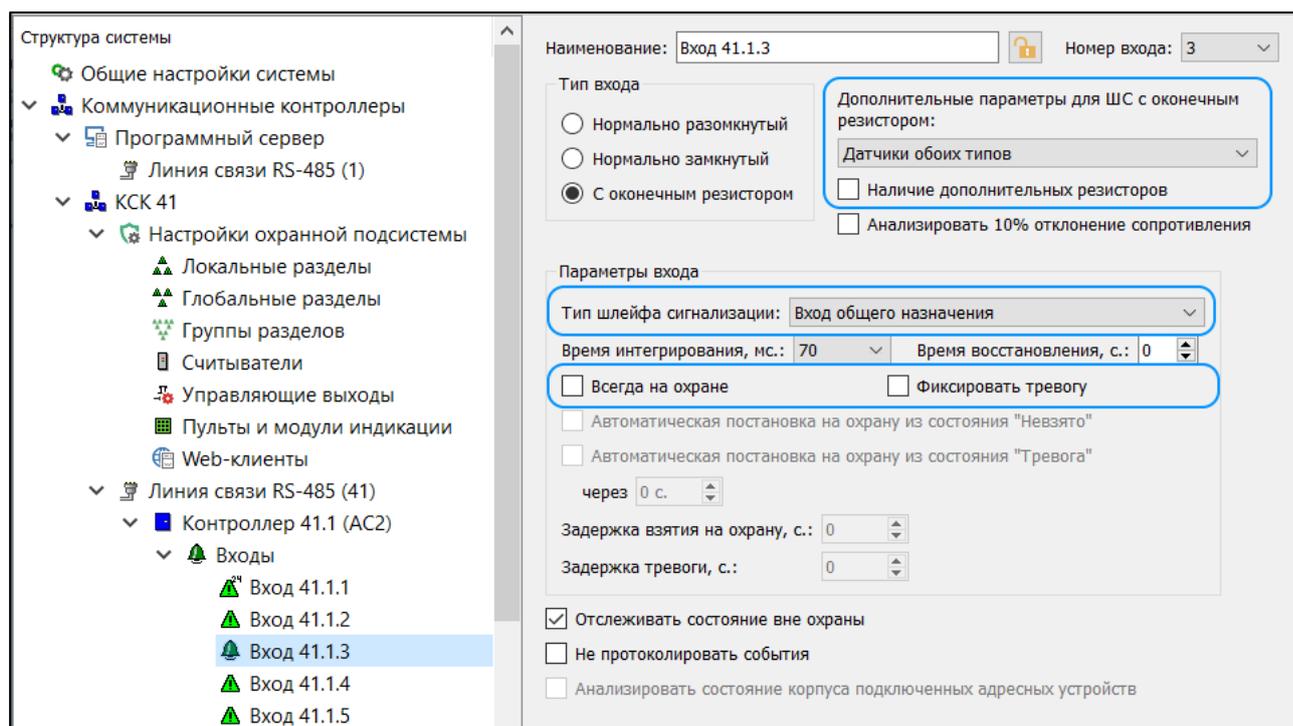


Рисунок 4. Дополнительные параметры входа общего назначения

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). Остальные шесть режимов (с оконечным резистором) возможны только для аналоговых входов. Кроме того, для аналоговых входов с оконечным резистором доступна опция «Анализировать 10% отклонение сопротивления».

В качестве охранных входов следует использовать встроенные аналоговые входы контроллеров с подключенным оконечным резистором (режим «Оба типа датчиков с оконечным резистором») либо входы устройств АДЛС охранного

контроллера Elsys-АС2. Для входов устройств АДЛС группа настроек «Тип входа» не используется.

Группа настроек «Параметры входа» устанавливает совокупность параметров входа в зависимости от типа ШС.

Доступны следующие типы шлейфов охранной сигнализации:

- Вход общего назначения;
- Охранный;
- Входной;
- Объем;
- Круглосуточный.

Особенности работы и настройки каждого типа шлейфа приведены в таблице (Таблица 4).

Таблица 4  
Варианты настройки «Тип шлейфа сигнализации»

<b>Тип ШС- «Вход общего назначения»</b>
<p>Вход, имеющий тип ШС «Вход общего назначения», не может быть включён в раздел.</p> <p>Для задания логики работы входа, имеющего этот тип ШС, следует использовать настройки «Всегда на охране» и «Фиксировать тревогу». При этом вход общего назначения может иметь четыре варианта конфигураций (см. Таблица 5).</p>
<b>Тип ШС- «Охранный»</b>
<p>Установка типа «Охранный» предусматривает использование входа в охранной подсистеме.</p> <p>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.</p> <p>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</p>

«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 перейдет в состояние «Тревога».

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.

На логику работы двери в подсистеме СКУД эти настройки не влияют.

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).

#### **Тип ШС- «Объём»**

Установка типа «Объём» предусматривает использование входа в охранной подсистеме.

Тип ШС «Объём» 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 «Объём» взаимосвязана с состоянием ШС типа «Входной», входящих в тот же раздел.

#### **Тип ШС- «Круглосуточный»**

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.

«Время интегрирования» – время, в течение которого контроллер детектирует переход входа из одного физического состояния в другое. Возможные значения параметра: 0, 70 или 300 мс.

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 от дребезга контактов);

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

«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».

«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 (Таблица 7) описана логика работы входа с типом ШС «Вход общего назначения» для различных комбинаций настроек «Всегда на охране» и «Фиксировать тревогу».

Таблица 5

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»	Логика 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».

Выбор опции «Автоматическая постановка на охрану из состояния «Не взято» обеспечивает переход входа в состояние «На охране», если ШС будет находиться в нормальном состоянии 3 с. Эта опция может быть установлена для следующих типов ШС: «Охранный», «Входной» и «Объем».

Выбор опции «Автоматическая постановка на охрану из состояния «Тревога» обеспечивает переход входа в состояние «На охране», если ШС после восстановления будет находиться в нормальном состоянии в течении времени, которое задается в диапазоне от 0 до 1250 с. Опция может использоваться для всех типов ШС кроме типа «Вход общего назначения».

Настройка «Задержка взятия на охрану» 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.

Настройка «Задержка тревоги» 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».

Установка опции «Не протоколировать события» доступна только для входа общего назначения и позволяет отключать регистрацию и передачу информации об изменении состояния входа.

Опция «Анализировать состояние корпуса подключенных адресных устройств» доступна только для входов устройств АДЛС и позволяет включать регистрацию и передачу информации об изменении состояния тампера крышки корпуса адресных устройств.

Логические состояния, поддерживаемые различными типами ШС приведены в таблице (см. Таблица 6).

Таблица 6.  
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	+	+	+	+	+	+	+	+
12	Нет связи	–	–	–	–	+	+	+	+
13	Взлом корпуса	–	–	–	–	+	+	+	+
14	Ошибка конфигурации	–	–	–	–	+	+	+	+

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;

№	Состояние	Тип ШС						
		1.1	1.2	1.3	1.4	2	3	4
1.4 – «Вход общего назначения», опция «Всегда на охране» – включена, опция «Фиксировать тревогу» – включена; 2 – «Охранный»; 3 – «Входной»; 4 – «Объём»; 5 – «Круглосуточный». Состояния 12 – 14 могут быть только у входов устройств АДЛС. Здесь и далее в этом документе используются эти сокращённые обозначения типов ШС.								

Состояния «Обрыв» и «Короткое замыкание» возникают при физических состояниях ШС, соответствующих неисправностям. Эти состояния возможны только для ШС типов 1.3 и 1.4.

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 оказался в нарушенном состоянии, будет сформировано состояние «Удержание».

### 2.3 Настройка локальных разделов

В контроллерах Elsys-AC2 может быть создано до 255 разделов охранной сигнализации. В раздел могут быть включены собственные ШС и адресные входы АДЛС.

В контроллерах Elsys-MB-AC, Elsys-MB, Elsys-NG-xx может быть создано до 8 разделов охранной сигнализации. В раздел могут быть включены входы, у которых установлен тип ШС, отличный от входа общего назначения.

В контроллерах Elsys-MB и Elsys-NG-xx в раздел могут быть включены также двери. Ворота и турникеты в раздел включены быть не могут. 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».

В контроллерах Elsys-MB и Elsys-NG-xx при участии двери в составе раздела возможно использование событий СКУД (штатный вход или штатный выход) для управления режимами охранной подсистемы. При этом для разделов могут использоваться следующие дополнительные опции:

- «Досрочная постановка на охрану после выхода»;
- «Автоматически снимать с охраны при входе в помещение»;
- «Автоматическая постановка на охрану при выходе последнего сотрудника».

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».

Вид окна настройки локального раздела приведён на рисунке (Рисунок 5).

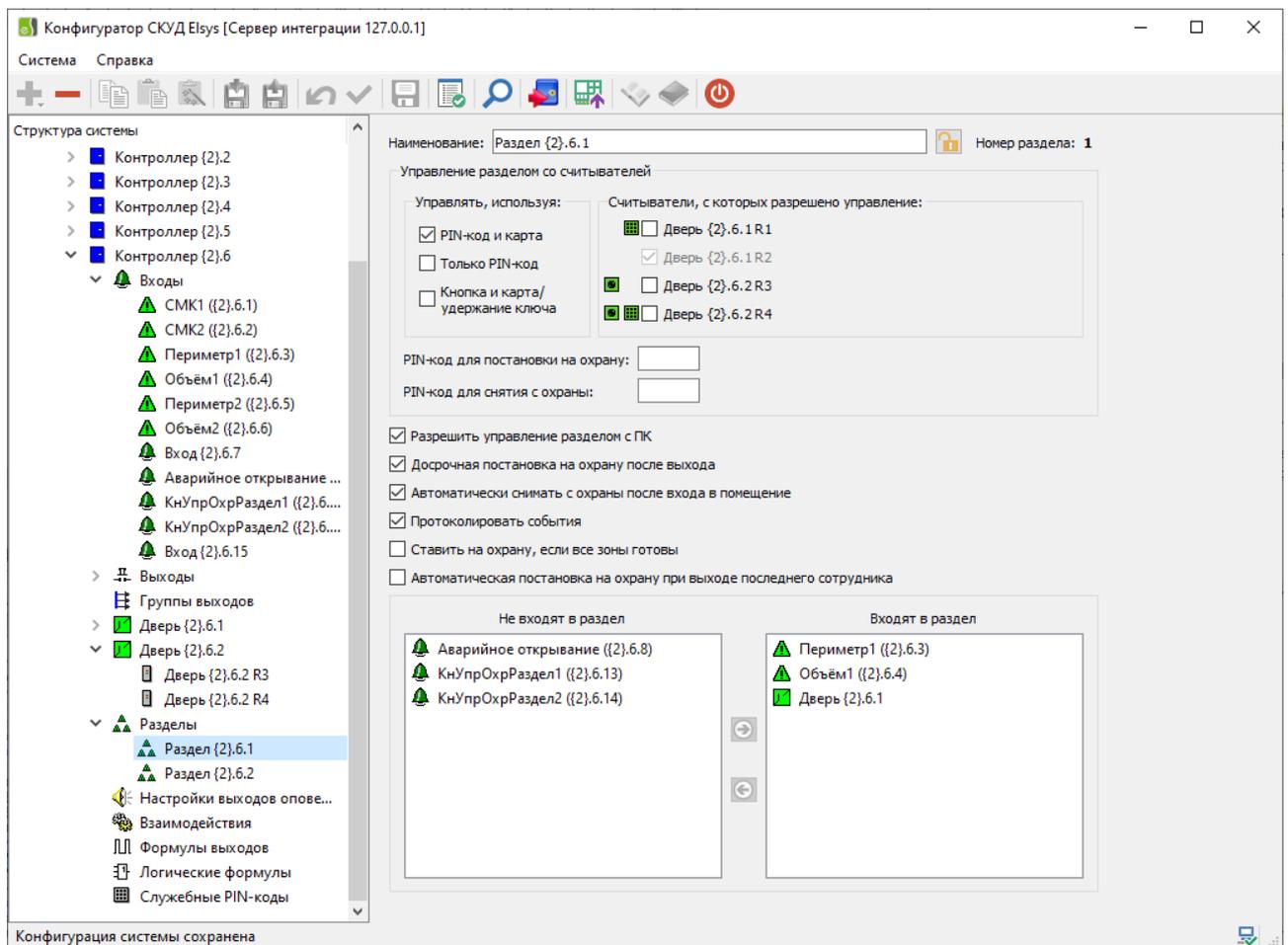


Рисунок 5. Окно настройки локальных разделов

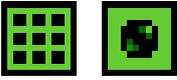
Настройки на фрейме «Управление разделом со считывателей» доступны при наличии в конфигурации контроллера хотя бы одного считывателя.

Группа настроек «Управлять, используя» содержит опции выбора способа управления режимами охраны с помощью считывателей. Описание возможных способов управления приведено в п. 4.1.

Группа настроек «Считыватели, с которых разрешено управление» позволяет назначить разделу считыватели, которыми будет осуществляться управление. Также будут отображаться пиктограммы (см. Рисунок 5) показывающие способ управления охраняемым разделом в зависимости от выбранных настроек охранного раздела в поле «Управлять, используя» и в поле «Использовать устройства» подключенного считывателя (см. Таблица 7).

Таблица 7.

Условия отображения пиктограмм у считывателей

Пиктограмма	Условия отображения
	В окне конфигурации считывателя в группе настроек «Использовать устройства» выбрана опция «Клавиатуру» или «Считыватель и клавиатуру».
	В окне конфигурации считывателя в группе настроек «Использовать устройства» выбрана опция «Считыватель». Назначен вход для подключения кнопки управления охранным разделом в окне основных настроек считывателя
	В окне конфигурации считывателя в группе настроек «Использовать устройства» выбрана опция «Считыватель и клавиатуру». Назначен вход для подключения кнопки управления охранным разделом в окне основных настроек считывателя.

Поля ввода «PIN-код для постановки на охрану» и «PIN-код для снятия с охраны» служат для установки PIN-кодов, с помощью которых выполняется управление разделом.

Добавление входов в раздел осуществляется путем переноса доступных входов из списка «Не входят в раздел» в список «Входят в раздел». Для удаления входов из раздела перенос осуществляется в обратном порядке.

Опция «Разрешить управление с ПК» включает (выключает) возможность управления разделом с компьютера с помощью команд, передаваемых по сетевому интерфейсу (RS-485 или Ethernet).

Опция «Досрочная постановка на охрану после выхода» 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.

Опция «Автоматическое снятие с охраны при входе в помещение» 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».

Опция «Протоколировать события» позволяет включать (выключать) регистрацию контроллером событий раздела.

Опция «Ставить на охрану, если все зоны готовы» 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 УУ→На охране».

Для ШС, имеющих задержку взятия, и находящихся в состоянии «Норма», будут зарегистрированы события вида «Вход УУ→Взятие на охрану с задержкой». Если же такой ШС находится в состоянии «Нарушено», будет сформировано событие «Вход УУ→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 перейдет 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 перейдет в состояние «Задержка тревоги». В иных случаях ШС типа «Объём» немедленно перейдет 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».

Опция «Автоматическая постановка на охрану при выходе последнего сотрудника» описана в п. 4.4.

Настройка полномочий пользователей описана в п. 4.7.

### **3 Настройка централизованного управления охранной сигнализацией**

#### **3.1 Совместимость оборудования СКУД Elsys с централизованным управлением охраной**

Для управления охранной подсистемой в централизованном режиме необходим КСК Elsys-MB-Net II, имеющий версию встроенного программного обеспечения не ниже 3.10, или Elsys-NG-Net II.

В централизованном управлении охраной могут участвовать:

- охранные контроллеры Elsys-MB-AC версий не ниже 2.02;
- охранные контроллеры Elsys-AC2;
- клавиатуры Elsys-CP2;
- контроллеры доступа Elsys-MB, оснащённые модулем расширения памяти и имеющие версию встроенного программного обеспечения не ниже 2.69;
- контроллеры доступа Elsys-NG-xx.

Для этих контроллеров доступен следующий функционал:

- использование встроенных входов для организации охранных зон, участвующих в глобальных разделах;
- использование локальных разделов для централизованного мониторинга и управления;
- использование встроенных выходов в качестве выходов оповещения централизованной охранной сигнализации.

Для подключения контроллеров Elsys-MB через локальную компьютерную сеть Ethernet необходимы модули Elsys-IP версии не ниже 2.04.

Для охранных контроллеров Elsys-MB-AC и Elsys-AC2 возможно использование встроенного считывателя (как со встроенной клавиатурой, так и без неё) для централизованного управления охраной. В контроллерах Elsys-MB и Elsys-NG-xx использование считывателей для централизованного управления охраной недоступно.

Контроллеры иных версий и вариантов исполнения (Elsys-MB предыдущих вариантов исполнения, Elsys-IO/MB, Elsys-MB-SM и др.), не участвующие в работе охранной подсистемы, могут использоваться в общих линиях связи с устройствами, участвующими в централизованной охранной сигнализации.

### 3.2 Общие настройки

Перед началом конфигурирования сегмента централизованной охранной подсистемы следует выполнить общую настройку системы – добавить и настроить охранные контроллеры и контроллеры доступа, настроить входы, выходы, локальные разделы и т. д.

Если в охранной подсистеме предполагается использовать устройства, подключенные через локальную компьютерную сеть Ethernet, следует создать сетевую группу и назначить для неё в качестве устройства, осуществляющего опрос сетевой группы, ЦКОС (Elsys-MB-Net II или Elsys-NG-Net II). Все устройства, подключаемые по Ethernet и участвующие в этом сегменте охранной подсистемы, следует добавлять в эту сетевую группу (см. Рисунок 6).

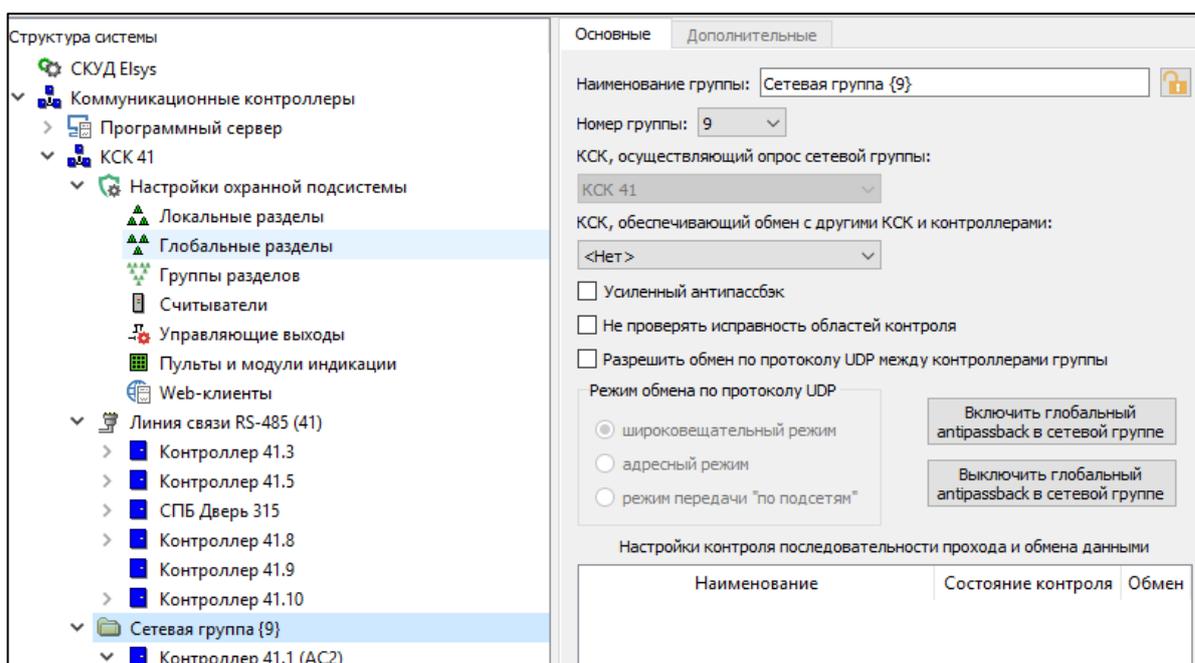


Рисунок 6. Настройки сетевой группы для централизованного управления

### 3.3 Настройка разделов и групп разделов

Список разделов формируется в конфигураторе оборудования SKUD Elsys, загружается в энергонезависимую память КСК и используется для обеспечения логики работы централизованного управления охранной сигнализацией.

Основные свойства разделов ЦКОС описаны в таблице (Таблица 8).

Таблица 8.  
Свойства разделов ЦКОС

	Свойство	Описание
1	Номер раздела	Числовое значение в диапазоне 1 – 9999, идентифицирующее раздел в пределах сегмента охранной сигнализации и используемое при управлении со считывателей, имеющих встроенную клавиатуру
2	Имя раздела	Текстовое значение (до 40 символов), используемое для идентификации раздела при его конфигурировании, мониторинге и управлении с точек управления охраной, имеющих текстовый или графический интерфейс
3	Тип раздела	Возможные варианты значения – «Глобальный», «Локальный» и «Группа разделов».

	Свойство	Описание
		<p>Глобальный раздел – раздел, содержащий охранные зоны различных приборов.</p> <p>В список разделов, участвующих в централизованном управлении охраной, могут быть добавлены локальные разделы охранных контроллеров Elsys-MB-AC и Elsys-AC2 и контроллеров доступа Elsys-MB и Elsys-NG-xx (тип раздела – «Локальный»). Формирование логического состояния таких разделов и регистрацию событий, отображающих изменение их состояния, осуществляют охранные контроллеры, в состав которых они входят, а разграничение полномочий и управление осуществляет центральный контроллер охранной сигнализации. Управление режимами охраны этих разделов и отображение их состояний могут осуществлять любые устройства, участвующие в централизованной охранной сигнализации (считыватели, блоки управления и индикации, выходы оповещения).</p> <p>Группа разделов может содержать локальные разделы и глобальные разделы.</p>
4	Состав раздела	<p>В состав раздела могут входить входы охранных контроллеров Elsys-MB-AC и Elsys-AC2 и контроллеров доступа Elsys-MB и Elsys-NG-xx.</p> <p>Для локальных разделов, добавленных в список разделов, обслуживаемых КСК, состав определяется настройками охранного контроллера.</p> <p>В состав группы разделов могут входить любые другие разделы, обслуживаемые КСК. Группы разделов в состав других групп входить не могут.</p>

Для добавления локальных разделов охранных приборов в список разделов, управляемых централизованно, следует использовать вкладку узла дерева устройств «КСК→Локальные разделы» (см. Рисунок 7).

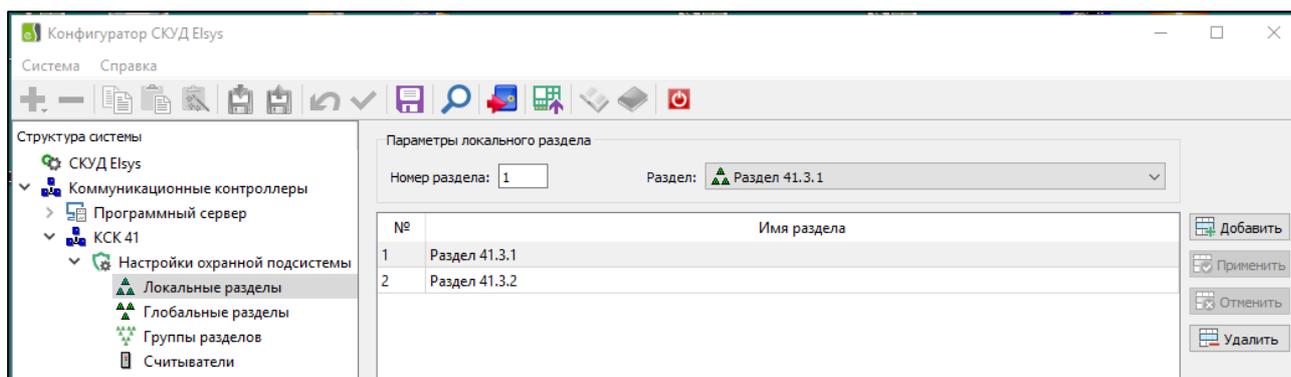


Рисунок 7. Окно настройки локальных разделов для централизованного управления

Для конфигурирования глобальных разделов следует использовать вкладку узла дерева устройств «КСК→Глобальные разделы» (см. Рисунок 8).

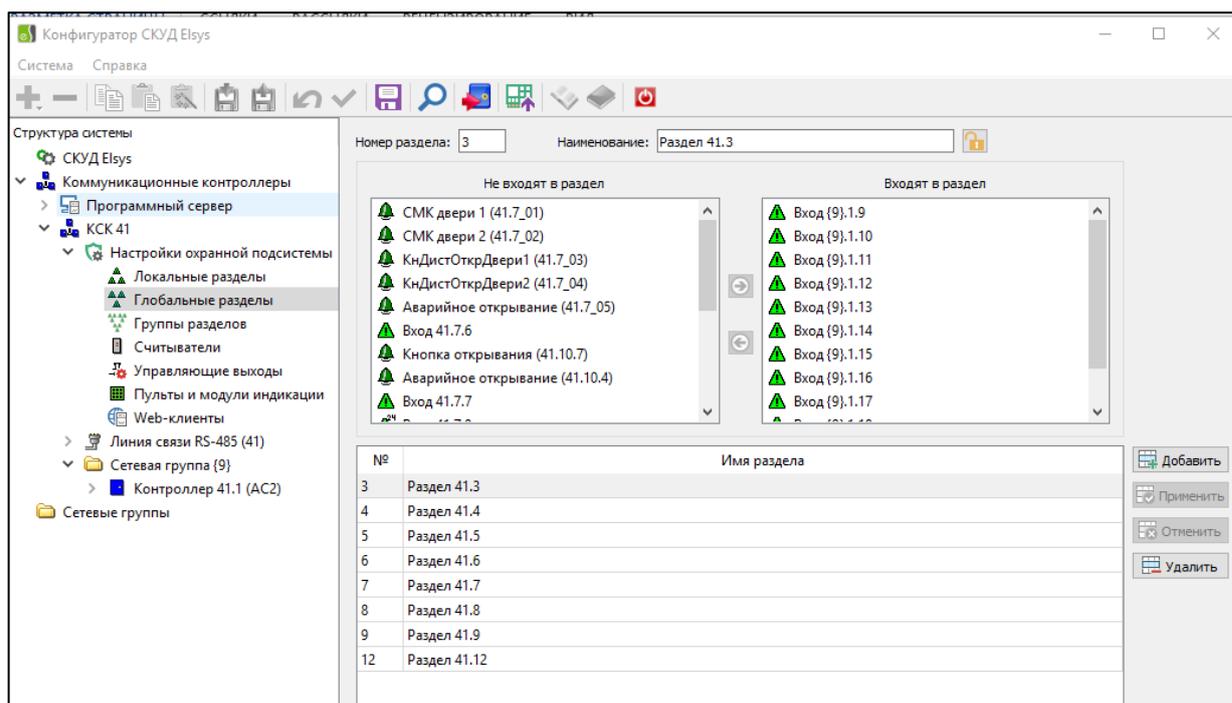


Рисунок 8. Окно настройки глобальных разделов

Для конфигурирования групп разделов следует использовать вкладку узла дерева устройств «КСК→Группы разделов» (см. Рисунок 9).

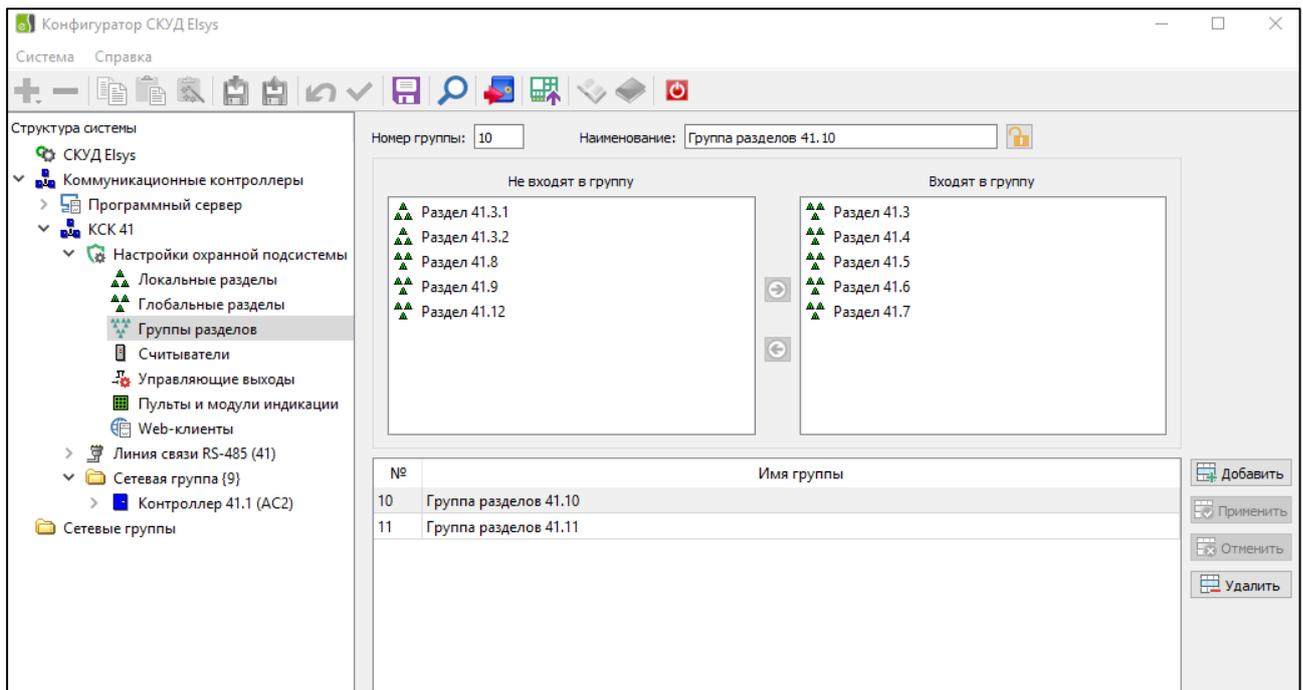


Рисунок 9 .Окно настройки групп разделов

### 3.4 Настройка считывателей для управления режимами охраны

Считыватели, участвующие в централизованном управлении охраной и подключенные к охранным контроллерам Elsys-MB-AC или Elsys-AC2, должны быть включены в список считывателей, обслуживаемых КСК. Для каждого из этих считывателей необходимо задать список разделов, которыми разрешено управлять с этого считывателя, либо разрешить управление всеми разделами, выбрав опцию «Разрешить управление всеми разделами».

Если считыватель оснащён клавиатурой, то в этом случае номер раздела вводится с клавиатуры, а список разрешённых разделов может использоваться для дополнительных ограничений полномочий. Если такие ограничения не требуются, следует выбрать опцию «Все разделы».

Если считыватель не оснащён клавиатурой, необходимо обеспечить, чтобы для каждого пользователя однозначно выбирался один и только один раздел, которым он будет управлять после предъявления карты. Для такого однозначного соответствия необходимо обеспечить, чтобы в состав любой группы управления охраной входило не более одного раздела, входящего в список разрешённых для этого считывателя. Если это условие не будет

выполнено, корректное управление охраной с такого считывателя будет невозможным.

**ВНИМАНИЕ!** Для обеспечения работы централизованного управления для считывателя охранного контроллера, не оснащённого клавиатурой, в свойствах считывателя в группе опций «Использовать устройства» необходимо выбрать опцию «Считыватель», а если считыватель оснащён клавиатурой, необходимо выбрать опцию «Считыватель и клавиатуру».

Описанные в настоящем разделе настройки загружаются при инициализации оборудования в энергонезависимую память КСК. Кроме того, информация об участии считывателей в централизованном управлении охраной загружается также в энергонезависимую память охранных контроллеров. Для применения этих настроек необходимо выполнить инициализацию этих устройств.

Вид окна настройки считывателей для управления режимами охраны приведён на рисунке (Рисунок 10).

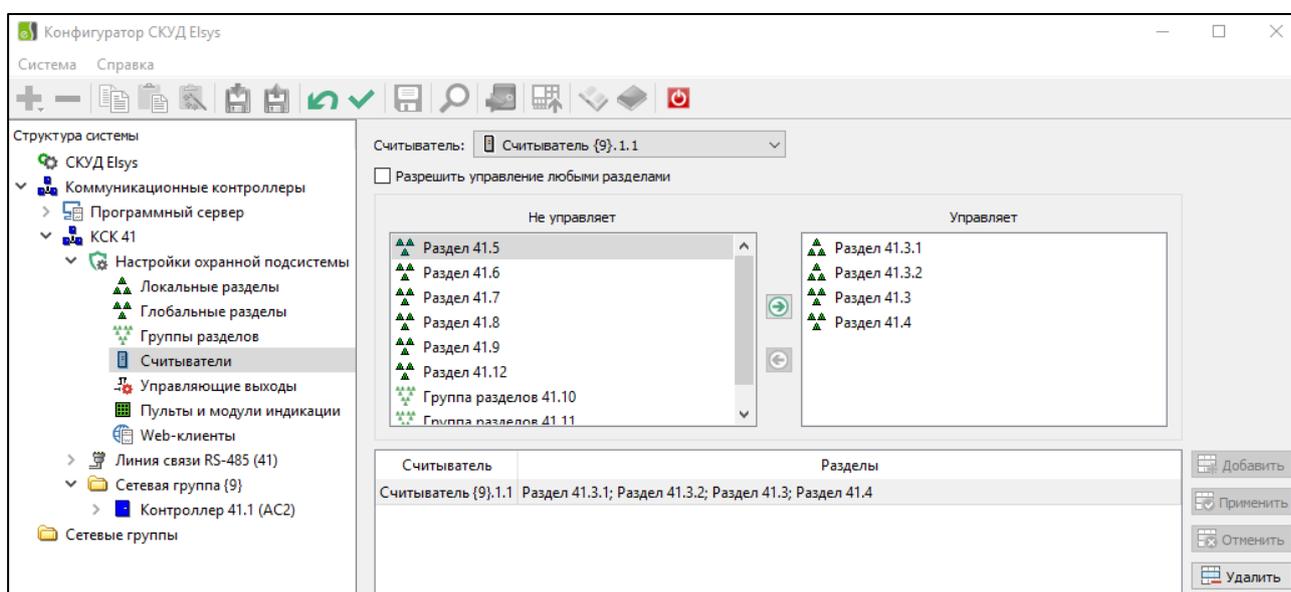


Рисунок 10. Окно настройки считывателей для управления режимами охраны

### 3.5 Настройка клавиатур Elsys-CP2

Для настройки работы клавиатур Elsys-CP2 следует в свойствах узла «Контроллер» выбрать требуемый режим работы – «Клавиатура» или «Управление и индикация».

Также при необходимости следует задать другие настройки (см. Рисунок 11, Рисунок 12):

- интерфейс считывателя;
- идентификация пользователя;
- отображение номеров индикаторов;
- ориентация дисплея.

Если задан способ идентификации с использованием PIN-кода, следует в свойствах пропуска пользователей охранной сигнализации задать PIN-коды пользователей, а на вкладке «Управление охраной» (см. Рисунок 26) установить режим идентификации «По карте и PIN-коду».

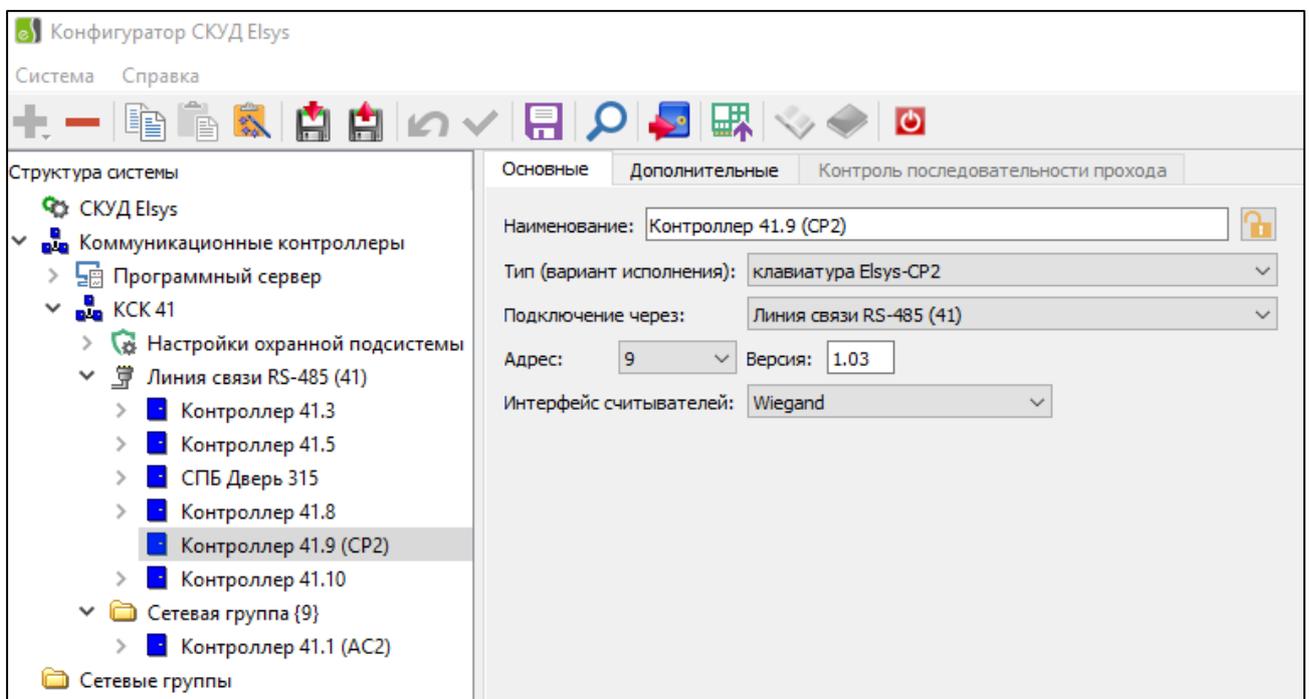


Рисунок 11 – Окно основных свойств клавиатуры Elsys-CP2

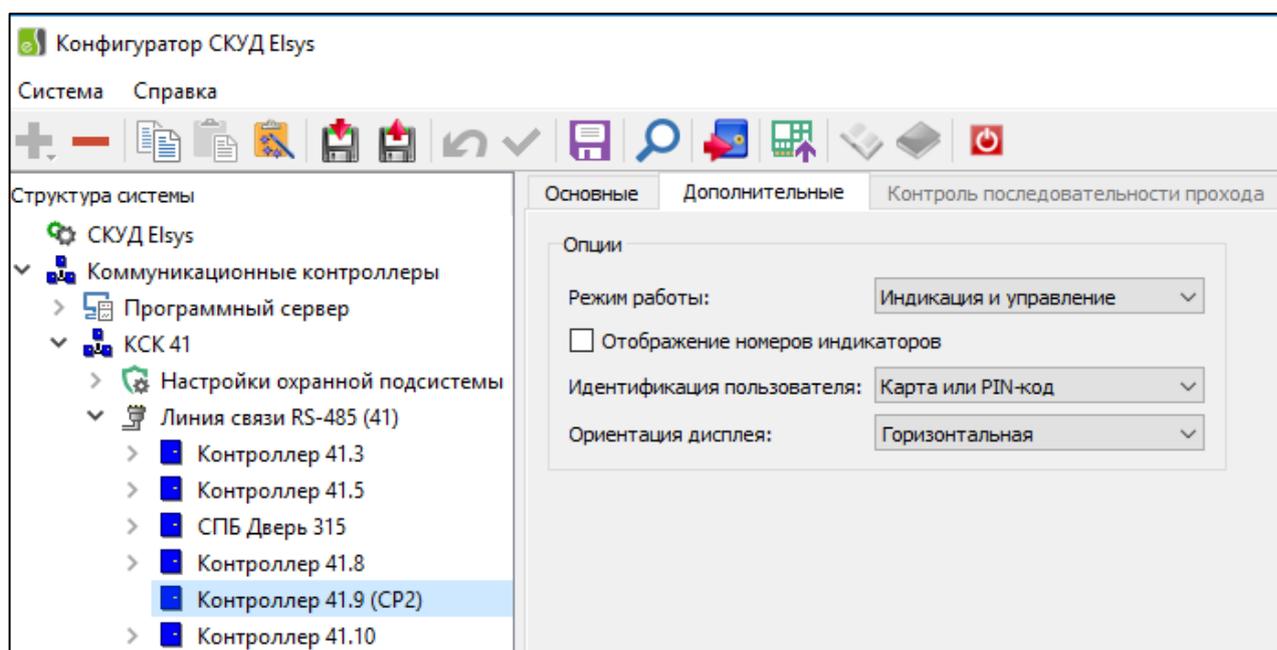


Рисунок 12. Окно дополнительных свойств клавиатуры Elsys-CP2

Если используется режим «Управление и индикация», следует в свойствах узла КСК «Пульты и модули индикации» назначить разделы или группы разделов для каждого из элементов управления и индикации клавиатуры Elsys-CP2. В качестве устройства для управления и индикации может быть выбран любой раздел или группа разделов из числа обслуживаемых этим КСК. Данные о разделах, назначенных для управления и индикации в клавиатурах Elsys-CP2, хранятся в энергонезависимой памяти КСК и используются им в оперативной работе.

Для загрузки настроек в память КСК и Elsys-CP2 следует выполнить инициализацию этих устройств.

На рисунке (Рисунок 13) приведён вид окна настройки пультов и модулей индикации.

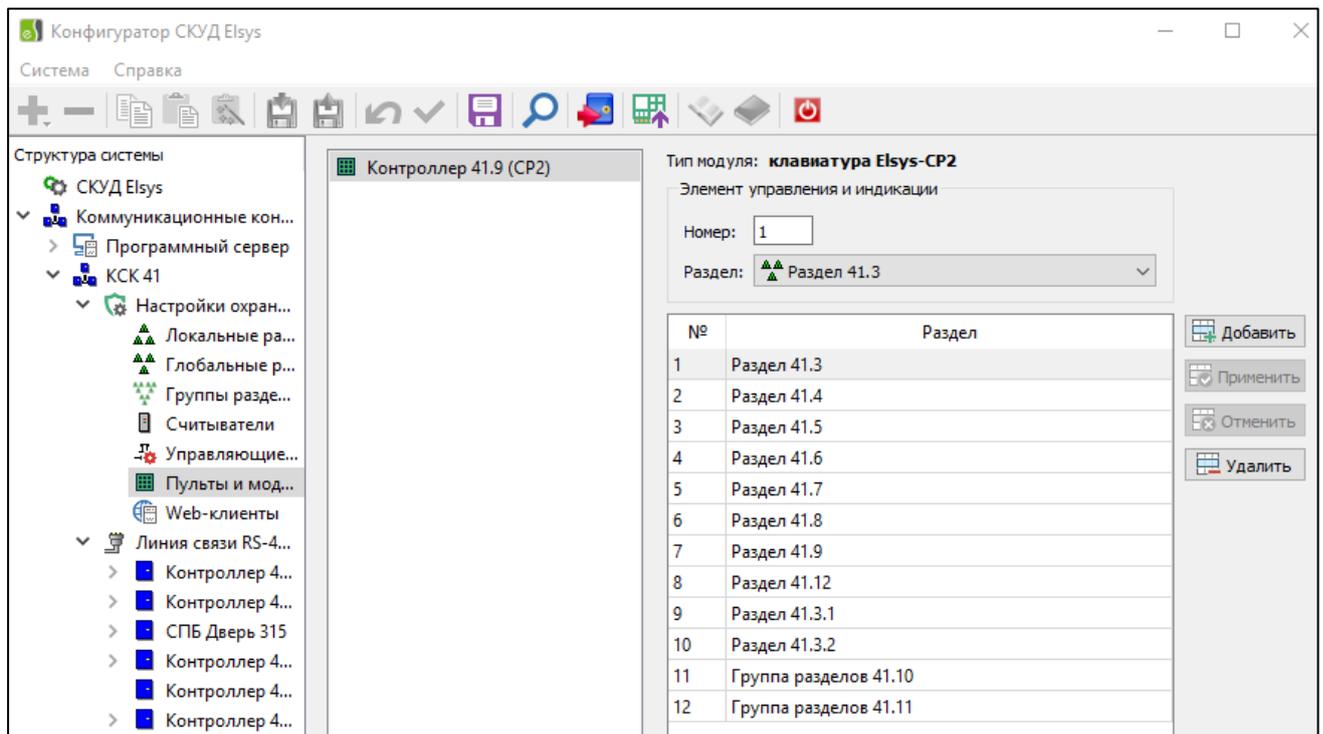


Рисунок 13 – Окно настройки пультов и модулей индикации

### 3.6 Настройка web-клиентов для управления режимами охраны

Web-клиент охранной подсистемы представляет собой сетевое рабочее место, выполняющее информационное взаимодействие с КСК и разворачиваемое на любом сетевом устройстве (ПК, планшет, мобильное устройство и др.), на котором может быть запущен web-браузер.

Для настройки управления охранной подсистемой через web-интерфейс следует использовать окно «КСК→web-клиенты» (см. Рисунок 14).

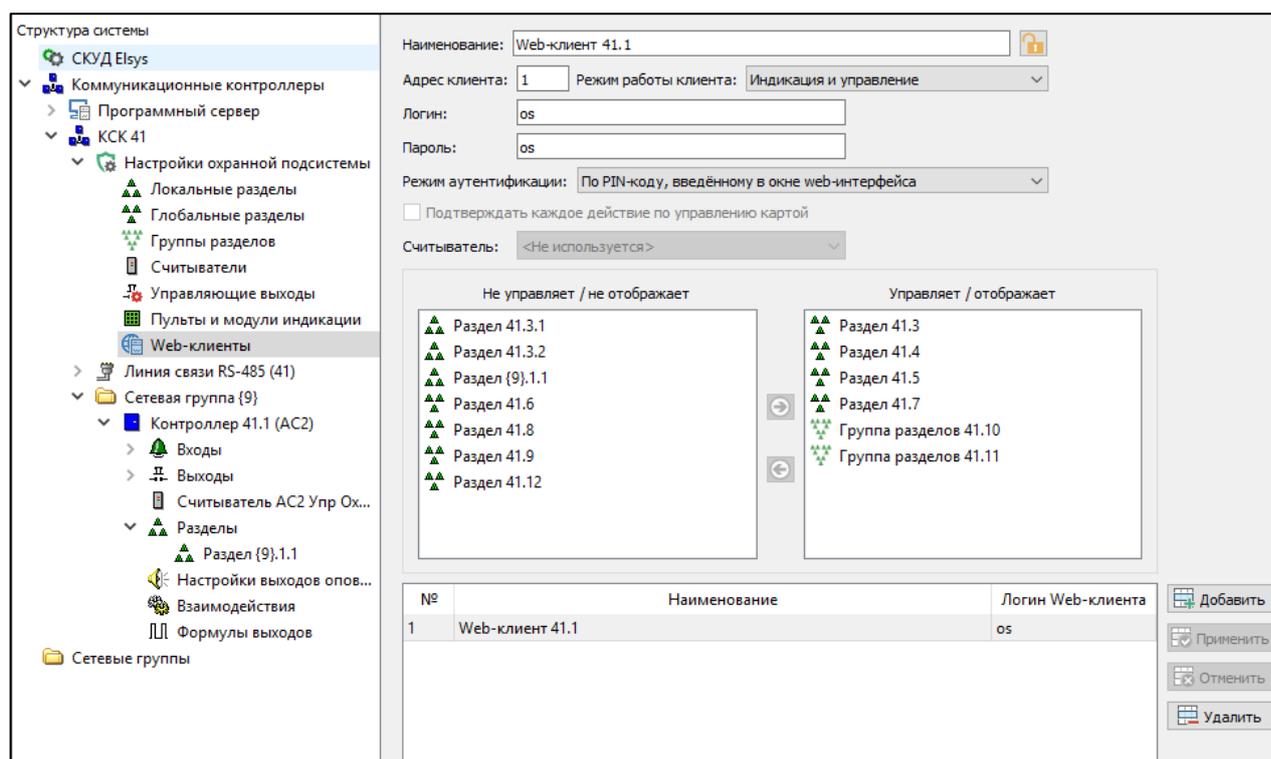


Рисунок 14 – Окно настройки web-клиентов

Для идентификации web-клиента используются логин и пароль, задаваемые в конфигураторе в соответствующих полях.

В поле «Наименование» задаётся имя web-клиента – его текстовый идентификатор в управляющем программном обеспечении.

Настройка «Режим работы клиента» может иметь значения:

- «Индикация и управление»;
- «Управление».

В режиме «Индикация и управление» на экран непрерывно выводятся состояния заданного набора разделов. После аутентификации пользователя охранной сигнализации в течение сеанса управления становятся доступными для выполнения постановки на охрану и снятия с охраны разделы, в соответствии с полномочиями пользователя.

В режиме «Управление» на экран на время сеанса управления выводится список разделов, соответствующий набору полномочий пользователя охранной сигнализации.

Настройка «Режим аутентификации» может иметь значения:

- «По карте со считывателя охранного контроллера»;

- «По PIN-коду, введённому в окне web-интерфейса»;
- «Управление без аутентификации»;
- «Индикация, управление недоступно».

Если установлено значение «По карте со считывателя охранного контроллера», необходимо задать считыватель, с которого будет выполняться аутентификация (поле ввода «Считыватель»). Дополнительно, может быть включена опция «Подтверждать каждое действие по управлению картой».

Если задан режим «Индикация и управление», следует сформировать список разделов, выводимых на экран web-клиента.

### 3.7 События и состояния

События охранной системы Elsys содержат тип, источник, время. Определить источник события можно до устройства, имеющего адрес (контроллер, вход, устройство АДЛС и т.д.). Некоторые события имеют дополнительные параметры, например № карты пользователя.

#### 3.7.1 *События контроллеров*

Контроллеры, участвующие в охранной системе Elsys, обеспечивают формирование событий, указанных в таблице (Таблица 9).

Таблица 9.  
События контроллеров

	<b>Текст события</b>	<b>Комментарии</b>
1	Взлом корпуса	
2	Восстановление зоны контроля взлома	
3	Потеря связи	
4	Восстановление связи	
5	Нарушение кольцевой топологии	Только для охранных контроллеров Elsys-AC2
6	Восстановление кольцевой топологии	Только для охранных контроллеров Elsys-AC2

#### 3.7.2 *События охранных зон*

Охранные контроллеры обеспечивают формирование событий, указанных в таблице (Таблица 10), от охранных зон.

Таблица 10  
События охранных зон

	Текст события	Комментарии
1	Норма (готов к взятию на охрану)	
2	Неготовность	
3	На охране	
4	Тревога	
5	Невзятие	
6	Снятие с охраны	
7	Задержка взятия	
8	Задержка взятия - неготовность	
9	Взлом корпуса	Только для устройств АДЛС
10	Восстановление зоны контроля взлома	Только для устройств АДЛС
11	Потеря связи	Только для устройств АДЛС
12	Восстановление связи	Только для устройств АДЛС
13	Неисправность	Только для устройств АДЛС

### 3.7.3 События считывателей

Коммуникационный сетевой контроллер обеспечивает формирование событий, указанных в таблице (Таблица 11), от считывателей участвующих в управлении охранной сигнализации.

Таблица 11.  
События считывателей

	Текст события	Комментарии
1	Отказ в доступе – нет полномочий	№ карты
2	Постановка на охрану	№ карты
3	Снятие с охраны	№ карты
4	Идентификация пользователя	№ карты
5	Восстановление связи со считывателем	Регистрируется устройством, к которому подключен считыватель
6	Потеря связи со считывателем	

### 3.7.4 События и состояния разделов

Разделы, обслуживаемые КСК, могут находиться в одном из перечисленных ниже логических состояний:

- «Тревога»;
- «Задержка тревоги» («Тревога входной зоны»);
- «Неисправность»;
- «На охране»;
- «Задержка постановки на охрану – неготовность»;
- «Задержка постановки на охрану – норма»;
- «Частично на охране, все зоны, снятые с охраны, готовы к постановке на охрану»;
- «Частично на охране, есть зоны в состоянии «Неготовность»;
- «Неготовность к постановке на охрану»;
- «Готовность к постановке на охрану».

Эти состояния передаются на клавиатуры Elsys-CP2 и считыватели, с которых выполняется управление охраной, а также используются для управления устройствами оповещения.

КСК регистрирует для глобальных разделов события, отображающие либо изменение логического состояния раздела, либо действия пользователей по управлению режимами охраны. Следует учитывать, что КСК не формирует отдельные события при изменении состояния «Готовность к постановке на охрану» на «Неготовность к постановке на охрану», и наоборот, однако передаёт текущее состояние раздела в управляющее программное обеспечение и для устройств индикации.

Список событий разделов приведён в таблице (Таблица 12).

Таблица 12.  
События разделов

	Текст события	Комментарии
1	Взятие на охрану	
2	Снятие с охраны	
3	Невзятие на охрану	
4	Взятие на охрану с задержкой	
5	Тревога входной зоны	
6	Тревога	
7	Неисправность	
8	Частично на охране	

	Текст события	Комментарии
9	Запрос на взятие	№ карты
10	Запрос на снятие	№ карты
11	Неисправность при взятии	
12	Неисправность при снятии	
13	Недоступно для управления	№ карты
14	Нет полномочий для взятия на охрану	№ карты
15	Нет полномочий для снятия с охраны	№ карты
16	Взятие на охрану пользователем	№ карты
17	Снятие с охраны пользователем	№ карты
18	Невзятие на охрану пользователем	№ карты

## 4 Управление режимами охраны

### 4.1 Локальное управление режимами охраны с помощью считывателей

Все возможные способы локального управления режимами охраны с помощью считывателей описаны в таблице (Таблица 13).

Таблица 13.

Способы управления режимами охраны с использованием считывателей

Способ управления режимом охраны	Описание
PIN-код и карта	Для использования этого способа в настройках раздела должна быть включена опция «PIN-код и карта». Этот способ нельзя использовать одновременно со способом «Только PIN-код». Считыватель должен быть оборудован клавиатурой. Должны быть заданы настройки «PIN-код для постановки на охрану» и «PIN-код для снятия с охраны» (эти PIN-коды могут совпадать). Для управления режимом охраны раздела необходимо ввести PIN-код, соответствующий локальному разделу и выбранному действию (постановка на охрану или снятие с охраны) и предъявить карту. Если пользователь имеет необходимые полномочия, считыватель отобразит текущее состояние раздела, после чего необходимо повторно предъявить карту. Команда управления будет сформирована в соответствии с

Способ управления режимом охраны	Описание
	<p>введённым PIN-кодом и полномочиями сотрудника. Если «PIN-код для постановки на охрану» и «PIN-код для снятия с охраны» совпадают, состояние раздела будет изменено на противоположное (если он был снят с охраны, выполнится постановка на охрану, а если был на охране, выполнится снятие с охраны).</p>
PIN-код	<p>Для использования этого способа в настройках раздела должна быть включена опция «Только PIN-код». Этот способ нельзя использовать одновременно со способом «PIN-код и карта». Считыватель должен быть оборудован клавиатурой. Должны быть заданы настройки «PIN-код для постановки на охрану» и «PIN-код для снятия с охраны» (эти PIN-коды могут совпадать). Для управления режимом охраны необходимо ввести соответствующий PIN-код, и, после отображения на индикаторе считывателя состояния выбранного раздела, набрать на клавиатуре символ «*».</p>
Карта	<p>Для использования этого способа у раздела должна быть включена опция «Карта».</p> <p>Для управления режимом охраны необходимо предъявить карту, имеющую необходимые полномочия, после чего на индикаторах считывателя отобразится состояние раздела, соответствующего полномочиям пользователя. 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>
Кнопка и карта	<p>Для использования этого способа у раздела должна быть включена опция «Кнопка и карта/ Удержание ключа». Кроме того, у считывателя, с которого предполагается выполнять управление режимами охраны, должна быть настроена кнопка управления режимом охраны, и должен быть назначен «Раздел для управления и мониторинга».</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>

Способ управления режимом охраны	Описание
Удержание ключа	Этот способ возможен, если считыватель подключен по интерфейсу 1-Wire (Touch Memory). Для использования этого способа у раздела должна быть включена опция «Кнопка и карта/ Удержание ключа». Кроме того, у считывателя должна быть включена опция «Анализировать удержание ключа/карты», и должен быть назначен «Раздел для управления и мониторинга». 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.
Примечание – Для режимов с использованием PIN-кодов для завершения ввода PIN-кода может использоваться вместо клавиши «*» клавиша «#», если в свойствах контроллера включена настройка «Завершать ввод клавишей #».	

Если считыватель оснащён клавиатурой, рекомендуется для всех разделов задавать способ управления «PIN-код и карта».

При использовании всех способов локального управления, кроме способа «PIN-код», контроллер анализирует полномочия сотрудников и обеспечивает авторизацию действий по управлению режимами охраны. После анализа полномочий контроллер в течение, примерно, 15 секунд индицирует на индикаторах считывателя состояние выбранного раздела. После выполнения управляющей команды отсчёт времени начинается заново. По истечении этого времени индикаторы считывателя переходят в исходное состояние. При наличии клавиатуры пользователь может досрочно завершить сеанс управления, нажав клавишу «#».

Если соответствующее действие разрешено, при постановке на охрану (снятии с охраны) будет сформировано событие типа «<Имя устройства> 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.

#### *4.1.1 Управление со считывателя охранного контроллера*

В настоящем разделе описано локальное управление режимами охраны с использованием считывателя для охранных контроллеров Elsys-MB-AC версий 2.02 и выше и Elsys-AC2. Более подробная информация содержится в руководствах по эксплуатации на эти контроллеры.

Локальное управление режимами охраны охранного контроллера с помощью считывателя возможно одним из трёх способов (см. Таблица 13):

- PIN-код и карта;
- PIN-код;
- Карта.

Если считыватель не оснащён клавиатурой, единственным способом локального управления является режим «Карта». Если используется режим «Карта», управление возможно только одним разделом (первым из списка разделов в наборе полномочий пользователя), поэтому при использовании этого режима для исключения неоднозначной работы следует в группу управления охраной пользователя добавлять не более чем один раздел охранного контроллера.

#### *4.1.2 Управление со считывателя контроллера доступа*

Для контроллеров доступа Elsys-MB и Elsys-NG-xx возможны следующие способы управления режимами охраны локальных разделов (см. Таблица 13):

- PIN-код и карта;
- PIN-код;
- Кнопка и карта;
- Удержание ключа.

### 4.2 Централизованное управление режимами охраны

#### *4.2.1 Управление со считывателя охранного контроллера*

Для участия считывателя, подключенного к охранному контроллеру, в централизованном управлении охраной, необходимо добавить его в список считывателей, обслуживаемых КСК, и сформировать список разделов, управление которыми должно быть доступно с этого считывателя.

Если считыватель контроллера не оснащён клавиатурой, то после предъявления карты контроллер сначала анализирует полномочия пользователя по локальному управлению охраной, и, если полномочия отсутствуют, отправляет запрос на управление центральному контроллеру.

Если считыватель контроллера оснащён клавиатурой, для управления глобальным разделом следует на клавиатуре дважды нажать клавишу «#», ввести номер глобального раздела, завершить ввод клавишей «\*» (если в свойствах контроллера включена настройка «Завершать ввод клавишей #», вместо клавиши «\*» следует использовать клавишу «#», и наоборот) и предъявить карту. После этого в КСК будет передан запрос на управление.

КСК, получив запрос на управление, анализирует полномочия пользователя по управлению запрошенным разделом и отправляет ответ охранному контроллеру, который отображает на индикаторах считывателя либо текущее состояние этого раздела, либо отказ в доступе на управление охраной. Одновременно КСК регистрирует событие – «Идентификация пользователя» (при наличии полномочий, см. Рисунок 15) либо «Отказ в доступе – нет полномочий» (при отсутствии полномочий).

При наличии полномочий по управлению разделом начинается сеанс управления этим разделом, в течение которого (примерно 15 секунд) контроллер отображает актуальное состояние этого раздела, а КСК при изменении состояния раздела передаёт контроллеру его новое состояние.

При предъявлении карты доступа в течение сеанса управления КСК выполняет действие по постановке раздела на охрану или по снятию с неё (если раздел был снят с охраны, выполнится постановка на охрану, а если был на охране, выполнится снятие с охраны). При этом сеанс управления охраной продлится ещё примерно на 15 секунд. По окончании выполнения команды на индикаторах считывателя будет отображён кратковременной индикацией результат выполнения команды («Взятие», «Снятие», «Невзятие»), после чего до окончания сеанса управления не будет отображаться новое состояние раздела.

Если считыватель оснащён клавиатурой, то досрочно завершить сеанс управления пользователь может, нажав клавишу «#».

На рисунке (Рисунок 15) показана последовательность событий, регистрируемых КСК и охранним контроллером при централизованном управлении охраной локального раздела «Раздел {9}.1.1», в состав которого входят зоны «Вход {9}.1.6» и «Вход {9}.1.8».

В начале сеанса управления, после проверки полномочий пользователя, КСК регистрирует событие «Считыватель →Идентификация пользователя».

В момент управления охраной КСК регистрирует два события – «Считыватель АС2 Упр Охраной{9}.1.1→ Постановка на охрану» и «Раздел {9}.1.1→ Запрос на взятие».

Затем, КСК транслирует команду для взятия раздела на охрану контроллеру, обслуживающему локальный раздел. После того, как контроллер выполнит эту команду и зарегистрирует события «Вход {9}.1.6→ На охране», «Вход {9}.1.8→ На охране», «Раздел {9}.1.1→ На охране» и передаст их в КСК, КСК передаёт результат выполнения в контроллер, с которого выполнялось управление. Также КСК, в дополнение к событию «Раздел {9}.1.1→ На охране», сформированному контроллером, регистрирует событие «Раздел {9}.1.1→ Взятие на охрану пользователем», содержащее информацию о пользователе, который ставил раздел на охрану.

```
12:37:49 Считыватель АС2 Упр Охраной{9}.1.1: Идентификация пользователя Зайцев Михаил
12:37:52 Считыватель АС2 Упр Охраной{9}.1.1: Постановка на охрану Зайцев Михаил
12:37:52 Раздел {9}.1.1: Запрос на взятие Зайцев Михаил
12:37:52 Раздел {9}.1.1: Взятие на охрану пользователем Зайцев Михаил
12:37:52 Вход {9}.1.6: На охране
12:37:52 Вход {9}.1.8: На охране
12:37:52 Раздел {9}.1.1: Взятие на охрану
```

Рисунок 15 – Последовательность событий при централизованном управлении режимом охраны локального раздела

На рисунке (Рисунок 16) показана последовательность событий, регистрируемых КСК и охранним контроллером при централизованном управлении охраной глобального раздела «Раздел 41.4», в состав которого входят зоны «Вход {9}.1.20» и «Вход {9}.1.21». Отличие от предыдущего варианта в том, что КСК формирует команды управления не для локального раздела, а для двух охранных зон, и затем, на основе событий, полученных от

контроллера ««Вход {9}.1.20»→На охране» и ««Вход {9}.1.21»→На охране» формирует состояние глобального раздела и регистрирует событие «Раздел 41.4→Взятие на охрану» с привязкой к имени пользователя.

13:00:53	Считыватель АС2 Упр Охраной{9}.1.1: Идентификация пользователя Зайцев Михаил
13:00:54	Вход {9}.1.20: На охране
13:00:54	Вход {9}.1.21: На охране
13:00:54	Считыватель АС2 Упр Охраной{9}.1.1: Постановка на охрану Зайцев Михаил
13:00:54	Раздел 41.4: Запрос на взятие Зайцев Михаил
13:00:54	Раздел 41.4: Взятие на охрану Зайцев Михаил

Рисунок 16 – Последовательность событий при централизованном управлении режимом охраны глобального раздела

#### 4.2.2 Использование клавиатуры Elsys-CP2

Клавиатура Elsys-CP2 предназначена для оперативного управления и отображения состояния охранных разделов в составе централизованной системы охраны, работающей под управлением ЦКОС.

В клавиатуре предусмотрены два режима работы:

- «Клавиатура»;
- «Индикация и управление».

Режим «Клавиатура» обеспечивает управление охранными разделами в рамках полномочий пользователя, выполнившего авторизацию. В состоянии ожидания клавиатура отображает заставку. После авторизации пользователя на экране отображается список разделов, которыми он имеет право управлять. В зависимости от назначенных полномочий, для каждого раздела доступны команды «Взять на охрану» и «Снять с охраны». На экране отображается до восьми элементов в виде продолговатых кнопок-пиктограмм с текстовыми именами разделов. Характер мигания и цвет кнопок соответствует состояниям отображаемых разделов. Предусмотрены элементы для пролистывания списка, если он не умещается на экране (полоса прокрутки). Кроме того, предусмотрена возможность непосредственного ввода номера раздела для управления.

Режим «Индикация и управление» предусматривает непрерывный вывод на экран заранее назначенного набора разделов. В этом режиме на экране отображается до 40 кнопок-пиктограмм с номерами разделов. Характер мигания и цвет кнопок соответствует состояниям отображаемых разделов. Пользователь,

выполнивший авторизацию, имеет право управлять охранными разделами из этого списка, в соответствии с назначенными ему полномочиями. В верхней части экрана расположены четыре индикатора статуса, отображающие общее интегрированное состояние разделов («Норма», «Тревога», «Нарушение», «Неисправность»), а также кнопка выключения звука.

В обоих режимах предусмотрено автоматическое завершение сеанса управления через 15 с после прекращения активности пользователя, а также принудительное завершение сеанса управления по кнопке.

Для обоих режимов может быть установлено свойство «Ориентация экрана», предусматривающее два значения:

- «Вертикальная»;
- «Горизонтальная».

Для режима «Индикация и управление» предусмотрена настройка «Отображение номеров индикаторов». Если она включена, на кнопках-пиктограммах отображаются номера индикаторов (числовые значения от 1 до 24), а если выключена – номера разделов (числовые значения в диапазоне 1 – 9999).

Для корректного отображения имён и номеров разделов они должны быть предварительно загружены в клавиатуру из управляющего программного обеспечения.

На рисунке (Рисунок 17) показана последовательность событий, регистрируемых КСК и охранным контроллером при централизованном управлении охраной с клавиатуры Elsys-CP2 для глобального раздела «Раздел 1.3», в состав которого входит зона «Вход 1.1\_01».

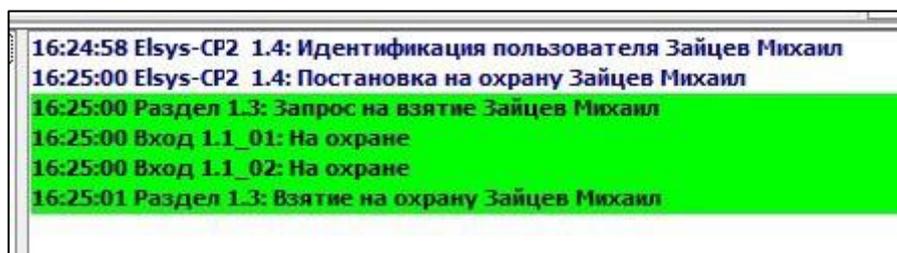


Рисунок 17 – Последовательность событий при централизованном управлении режимом охраны глобального раздела с клавиатуры Elsys-CP2

### 4.2.3 Управление через web-интерфейс браузера

Для начала сеанса работы через web-интерфейс следует ввести в браузере строку вида:

<IP-адрес КСК>/ops/<Логин web-клиента> (см. Рисунок 18).

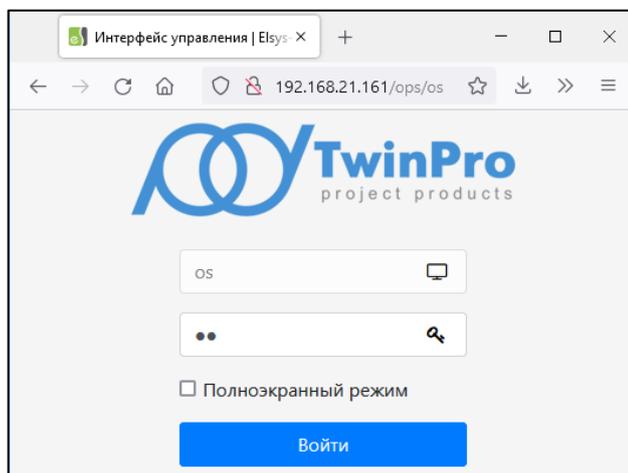


Рисунок 18 – Начало сеанса работы через web-интерфейс

На приведённом выше рисунке IP-адрес КСК – «192.168.21.161», логин web-клиента – «os».

Далее, после успешного ввода пароля web-клиента, в зависимости от заданного в настройках режима работы, будет выведено либо окно с настроенным для этого web-клиента списком разделов (Рисунок 19), либо окно ожидания аутентификации по PIN-коду (Рисунок 20) или карте (Рисунок 21).

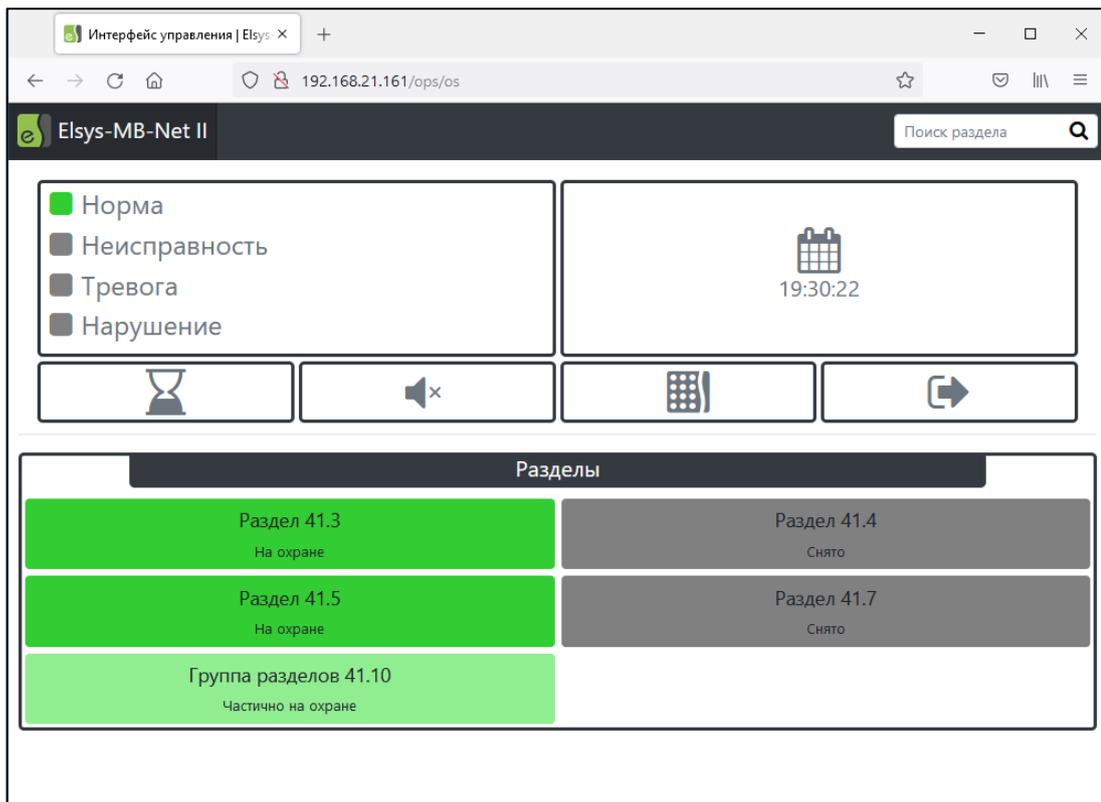


Рисунок 19 – Окно web-клиента в режиме «Индикация и управление»

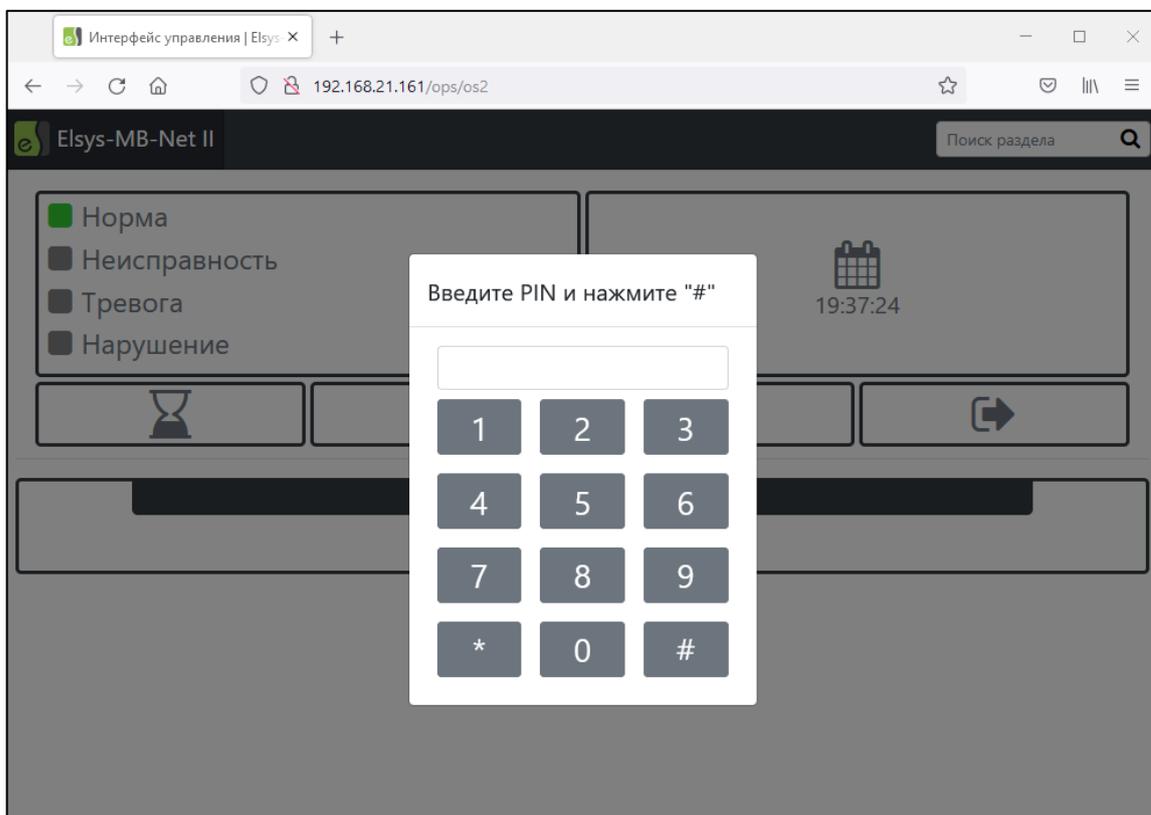


Рисунок 20 – Окно web-клиента в режиме «Управление» (идентификация по PIN-коду)

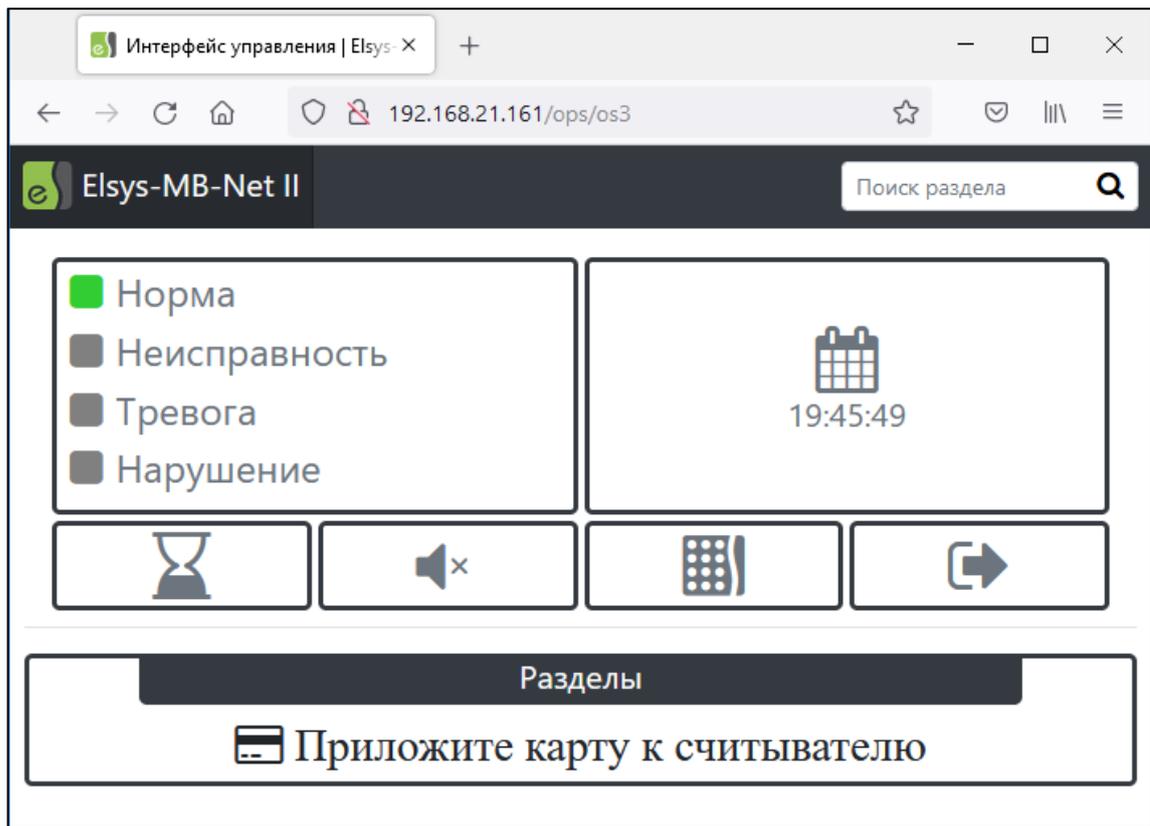


Рисунок 21 – Окно web-клиента в режиме «Управление» (идентификация по карте)

Окно web-клиента в режимах «Управление» и «Управление и индикация» имеет схожий вид. В верхней части экрана расположена панель с индикаторами «Норма», «Неисправность», «Тревога», «Нарушение», отображающими интегрированное состояние выводимых для индикации разделов (см. Рисунок 22).

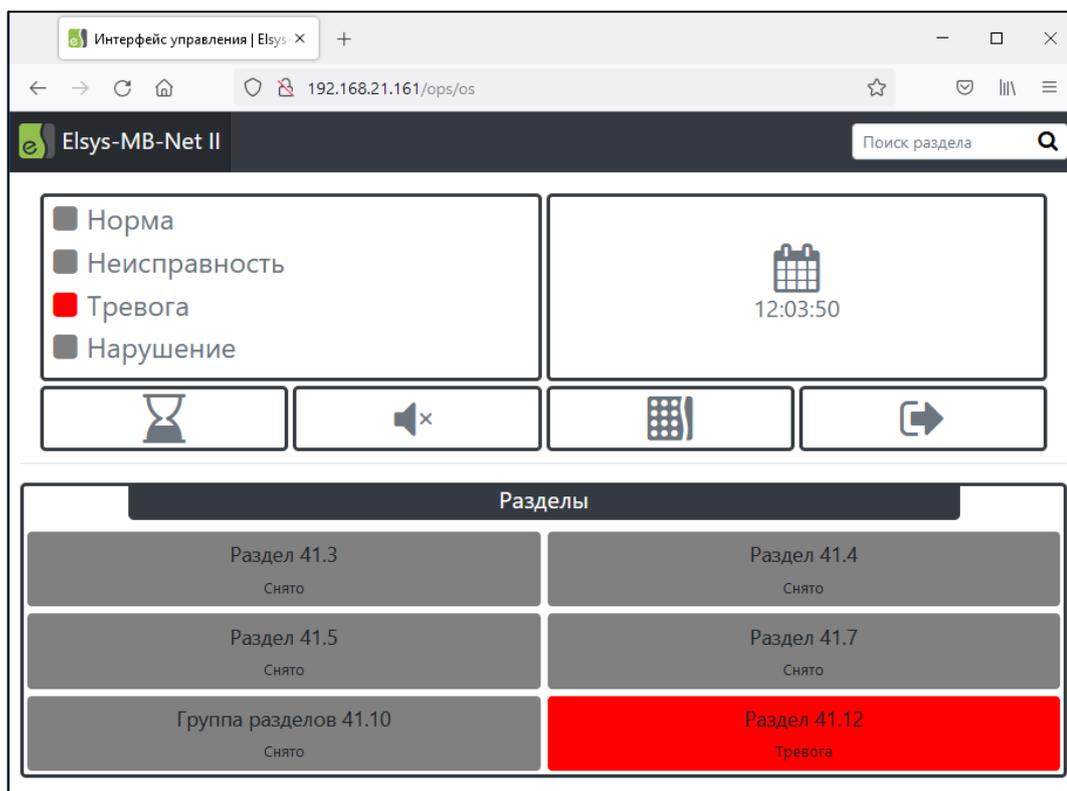


Рисунок 22 – Отображение интегрированного состояния индицируемых разделов

Индикатор  служит для отображения процесса выполнения команд.

Кнопка  предназначена для отключения звукового сопровождения текущей принятой тревоги.

Для аутентификации в режиме «Индикация и управление» следует, в зависимости от настроек web-клиента, либо предъявить карту считывателю охранного контроллера, либо ввести PIN-код в окне ввода, вызываемом кнопкой .

В режиме «Управление» (Рисунок 20, Рисунок 21) следует выполнить аутентификацию, введя PIN-код или предъявив карту считывателю охранного контроллера.

После аутентификации пользователя в течение сеанса управления становятся доступными элементы управления (кнопки разделов и соответствующие им пункты меню «Взять», «Снять»), в соответствии с настройками группы управления охраной, назначенной пользователю. Сеанс

управления длится 30 секунд и продлевается на 30 с после каждого действия пользователя.

Кнопка  предназначена для досрочного завершения сеанса управления.

В режиме «Управление и индикация» или в течение сеанса управления в режиме «Управление» в основной части экрана находятся кнопки с названиями разделов, подписями и цветовыми схемами, обозначающими их логическое состояние.

Тревожные состояния и состояния, соответствующие неисправностям, отображаются в мигающем режиме со звуковым сопровождением. В этих состояниях синхронно с миганием индикаторов разделов мигают соответствующие индикаторы состояний («Нарушение», «Тревога», «Неисправность»).

Алгоритмы индикации состояний разделов в web-приложении описаны в таблице (Таблица 14).

Таблица 14.  
Индикация состояний разделов в web-приложении

Состояние раздела	Алгоритм индикации
Тревога	Мигание цвета фона синхронно со звуковым сигналом с частотой 2,5 Гц (0,2 с красный, 0,2 с серый, звуковой сигнал – 0,2 с включено, 0,2 с выключено)
Задержка тревоги	Мигание цвета фона синхронно со звуковым сигналом с частотой 1 Гц (0,5 с красный, 0,5 с серый, звуковой сигнал – 0,1 с включено, 0,9 с выключено)
Неисправность	Мигание цвета фона синхронно со звуковым сигналом с частотой 1 Гц (0,5 с жёлтый, 0,5 с серый, звуковой сигнал – 0,1 с включено, 0,9 с выключено)
Задержка взятия на охрану – неготовность	Цвет фона светло-зелёный, на изображении присутствует диагональная красная полоса
На охране	Цвет фона зелёный
Задержка взятия на охрану	Цвет фона светло-зелёный
Частично на охране – неготовность	Цвет фона светло-зелёный, на изображении присутствует диагональная фиолетовая полоса
Частично на охране	Цвет фона светло-зелёный
Неготовность	Цвет фона фиолетовый

Состояние раздела	Алгоритм индикации
Снято с охраны	Цвет фона серый
Примечание – Если одновременно индицируется несколько тревожных состояний, звуковой сигнал работает в соответствии с наиболее приоритетным из них.	

Для управления режимами охраны разделов следует путём нажатия соответствующей кнопки (с использованием мыши или сенсорного дисплея, в зависимости от устройства) вызвать меню (см. Рисунок 23) и выполнить необходимое действие (доступность пунктов меню определяется полномочиями пользователя по управлению охраной).

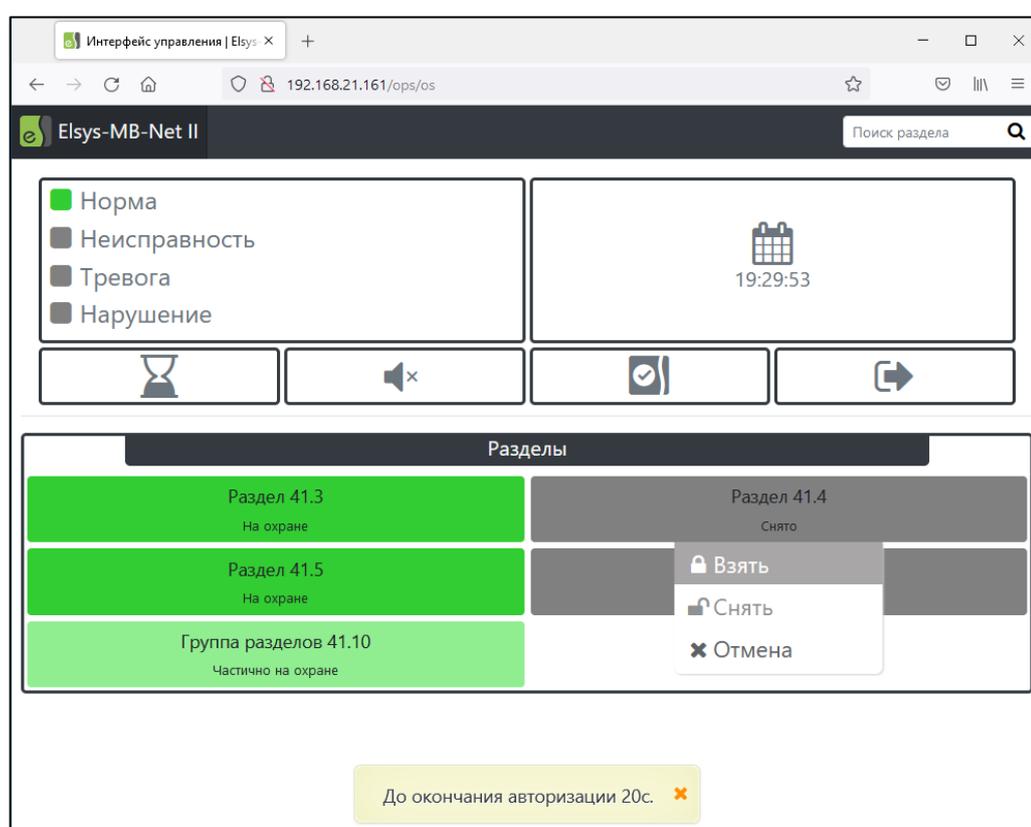


Рисунок 23 – Управление разделами через web-интерфейс

#### 4.3 Автоматизированное управление режимами охраны

В СКУД Elsys предусмотрено несколько способов автоматизированного управления режимами охраны локальных разделов и зон:

- автоматическое снятие раздела с охраны при входе в помещение первого сотрудника и автоматическая постановка раздела при выходе из помещения

последнего сотрудника (только для контроллеров доступа Elsys-MB и Elsys-NG-xx);

- управление режимами охраны зон и разделов через аппаратные взаимодействия;
- управление через программные сценарии управляющего программного обеспечения.

Подробно эти способы описаны в документации на управляющее программное обеспечение и оборудование.

Автоматическая постановка на охрану локального раздела описана в п. 4.4

#### 4.4 Автоматическая постановка на охрану при выходе последнего сотрудника

Для того, чтобы использовать эту функцию, необходимо включить одноимённую опцию раздела (Рисунок 5). 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 5);

- для раздела выключить настройку «Ставить на охрану, если все зоны готовы» (Рисунок 5);
- включить настройку раздела «Автоматическое снятие с охраны при входе в помещение» (Рисунок 5);
- 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 5).

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.

Нештатные ситуации, их причины и способы решения приведены в Таблица 15.

Таблица 15.

Описание нештатных ситуаций 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.

№	Описание ситуации	Причины	Способ решения
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 истечении 5 секунд 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.

#### 4.5 Управление с АРМ дежурного оператора

Управление режимами охраны отдельных входов (охранных зон) контроллера, локальных и глобальных разделов, а также групп разделов может осуществляться путём передачи контроллеру команд из управляющего программного обеспечения. Такие команды могут быть сформированы дежурным оператором поста охраны из контекстного меню пиктограммы устройства на графическом плане объекта (см. Рисунок 24).

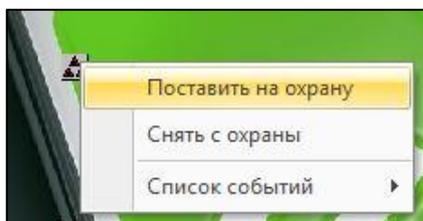


Рисунок 24 – Управление режимами охраны с графического плана объекта

**ВНИМАНИЕ!** Непосредственное управление режимами охраны отдельных входов (взятие на охрану и снятие с охраны) возможно при условии, что вход

не включен в состав раздела. Если вход включен в какой-либо раздел, управление его режимом возможно только в составе раздела.

#### 4.6 Алгоритмы индикации считывателей

Охранные контроллеры обеспечивают управление световой и звуковой индикацией считывателя (зелёный и красный светодиоды и звуковой излучатель) и отображение на этих индикаторах:

- событий, связанных с действиями пользователя по управлению охраной (предусмотрена кратковременная индикация, в течение 0,5 – 2 секунд);
- текущего состояния локального или глобального раздела, управление режимами которого выполняется в текущий момент (предусмотрена индикация в течение всего сеанса управления, в течение 15 секунд после последнего действия пользователя).

Индикация состояний локального или глобального раздела, выполняемая охранным контроллером Elsys-AC2, описана в таблице (Таблица 16).

Состояние раздела определяется наиболее высокоприоритетным состоянием среди ШС, входящих в состав раздела (наиболее высокому приоритету соответствует самое низкое числовое значение приоритета).

Таблица 16.  
Индикация состояний раздела

Приоритет состояния	Состояние	Алгоритм индикации
1	Тревога	Мигает красный и работает звуковой сигнализатор считывателя с частотой 2,5 Гц (по алгоритму «0,2 секунды включено / 0,2 секунды выключено»)
2	Неисправность ШС АДЛС	Мигает жёлтый и работает звуковой индикатор по алгоритму «0,1 секунды включено/0,9 секунды выключено»
3	Взлом корпуса для ШС АДЛС	Мигает красный и работает звуковой сигнализатор считывателя по алгоритму «три импульса по 0,1 секунды паузами по 0,1 секунды периодом 1 секунда»

Приоритет состояния	Состояние	Алгоритм индикации
4	Задержка тревоги	Мигает красный и работает звуковой сигнализатор считывателя по алгоритму «три импульса по 0,1 секунды паузами по 0,1 секунды периодом 1 секунда»
5	Невзятие	Мигает красный и работает звуковой сигнализатор считывателя по алгоритму «два импульса по 0,1 секунды паузами по 0,1 секунды периодом 1 секунда»
6	Задержка постановки на охрану – неготовность	Мигает красный и работает звуковой сигнализатор считывателя по алгоритму «два импульса по 0,1 секунды с паузами по 0,1 секунды периодом 1 секунда»
7	Задержка постановки на охрану – норма	Мигает красный и работает звуковой сигнализатор считывателя по алгоритму «0,1 секунды включено / 0,9 секунды выключено»
8	На охране	Включен красный
9	Неготовность охранного ШС	Непрерывно включен жёлтый
10	Неготовность ШС типа «Объём»	Мигает жёлтый по алгоритму «два импульса по 0,1 секунды с паузами по 0,1 секунды периодом 1 секунда»
11	Неготовность входного ШС	Мигает жёлтый по алгоритму «0,1 секунды включено / 0,9 секунды выключено»
12	Готовность	Включен зелёный

В контроллере Elsys-MB-AC используются те же алгоритмы индикации состояний разделов, что и в контроллере Elsys-AC2. Индикация состояний локальных разделов контроллерами Elsys-MB и Elsys-NG-xx имеет некоторые отличия и описана в документе «СКУД Elsys. Руководство по настройке».

В таблице (Таблица 17) описана индикация событий и действий по управлению режимами охраны для контроллера Elsys-AC2. После индикации события в течение 0,5 – 2 секунд световые индикаторы считывателя возвращаются к индикации состояния раздела, либо переходят в режим ожидания предъявления карты или отклика от центрального контроллера.

Таблица 17.  
Индикация считывателем событий и состояний,  
связанных с предъявлениями карт

№	Событие или действие	Звуковая индикация	Световая индикация
1	«Идентификация пользователя»	С задержкой в 0,4 секунды формируется импульс длительностью 0,3 секунды	Считыватель в течение примерно 12 секунд индицирует состояние раздела, управление которым может выполнять данный пользователь
2	«Неизвестная карта», «Отказ в доступе – нет прав»	С задержкой в 0,3 секунды формируются четыре импульса длительностью 0,1 секунды (паузы между импульсами составляют 0,1 секунды).	Синхронно с включением звукового сигнализатора светодиод мигает жёлтым цветом (четыре импульса длительностью 0,1 секунды, с паузами 0,1 секунды)
3	«Отказ в доступе – нет полномочий»	С задержкой в 0,3 секунды формируются три импульса длительностью 0,1 секунды (паузы между импульсами составляют 0,1 секунды).	Синхронно с включением звукового сигнализатора светодиод мигает жёлтым цветом (три импульса длительностью 0,1 секунды, с паузами 0,1 секунды)
5	«Постановка раздела на охрану»	С задержкой 0,3 секунды формируется импульс длительностью 0,5 секунды	Светодиод загорается красным. Считыватель в течение 12 секунд индицирует состояние раздела, управление которым выполнялось

№	Событие или действие	Звуковая индикация	Световая индикация
6	«Снятие раздела с охраны»	С задержкой в 0,3 секунды формируются два импульса длительностью 0,1 секунды, с паузой 0,1 секунды.	Синхронно с включением звукового сигнализатора светодиод мигает зелёным цветом (два импульса длительностью 0,1 секунды, с паузой 0,1 секунды). Считыватель в течение 12 секунд индицирует состояние раздела, управление которым выполнялось
7	«Неудачное взятие раздела на охрану»	С задержкой в 0,3 секунды формируются пять импульсов длительностью 0,1 секунды (паузы между импульсами составляют 0,1 секунды)	Синхронно с включением звукового сигнализатора светодиод мигает жёлтым цветом (пять импульсов длительностью 0,1 секунды, с паузами 0,1 секунды)
8	«Команда управления разделом игнорируется». (Например, в случае, если для снятого с охраны раздела подана команда «Снять с охраны»)	Нет звуковой индикации	Светодиод дважды вспыхивает жёлтым на 0,1 секунды, с паузой между импульсами 0,1 секунды.
9	Переход раздела из состояния «Задержка взятия» в состояние «На охране»	С задержкой 0,3 секунды формируется импульс длительностью 0,5 секунды	Световая индикация соответствует текущему состоянию раздела

№	Событие или действие	Звуковая индикация	Световая индикация
10	Ожидание ответа от КСК после запроса полномочий от КСК или запроса на выполнение управляющей команды при централизованном управлении охраной	Нет звуковой индикации	Светодиод мигает по алгоритму «0,1 секунды включен зелёный / 0,1 секунды включен жёлтый» в течение 12 секунд или до получения ответа от КСК.
11	Ожидание предъявления карты после ввода PIN-кода для авторизации управления локальным или глобальным разделом.	Нет звуковой индикации	Светодиод мигает зелёным (длительность импульса 0,1 секунды, паузы между ними 0,4 секунды) в течение 12 секунд

В контроллере Elsys-MB-AC используются те же алгоритмы индикации событий, что и в контроллере Elsys-AC2. Индикация событий при управлении локальными разделами контроллерами Elsys-MB и Elsys-NG-xx имеет некоторые отличия и описана в документе «СКУД Elsys. Руководство по настройке».

#### 4.7 Настройка полномочий пользователей по управлению режимами охраны

В централизованном режиме охраны, а также при локальном управлении охраной с использованием контроллеров Elsys-MB-AC и Elsys-AC2 следует в управляющем программном обеспечении настроить группы управления охраной и назначить их пользователям.

Окно настройки групп управления охраной показано на рисунке (Рисунок 25). Чтобы назначить полномочия пользователю необходимо в свойствах пропуска на вкладке «Управление охраной» указать соответствующую группу управления охраной (см. Рисунок 26).

При локальном управлении охраной с использованием контроллеров Elsys-MB и Elsys-NG-xx для настройки полномочий пользователей следует в

настройках профиля персонала включить индивидуальную опцию пользователя СКУД «Право постановки на охрану», а для разрешения снятия с охраны локальных разделов – опцию «Право снятия с охраны» (см. Рисунок 27).

Изменения списка пользователей и их полномочий загружаются в КСК и контроллеры автоматически, при условии, что в оборудовании содержится актуальная аппаратная конфигурация охранной подсистемы. При необходимости может быть выполнена полная загрузка в КСК и контроллеры списка пользователей и их полномочий (инициализация).

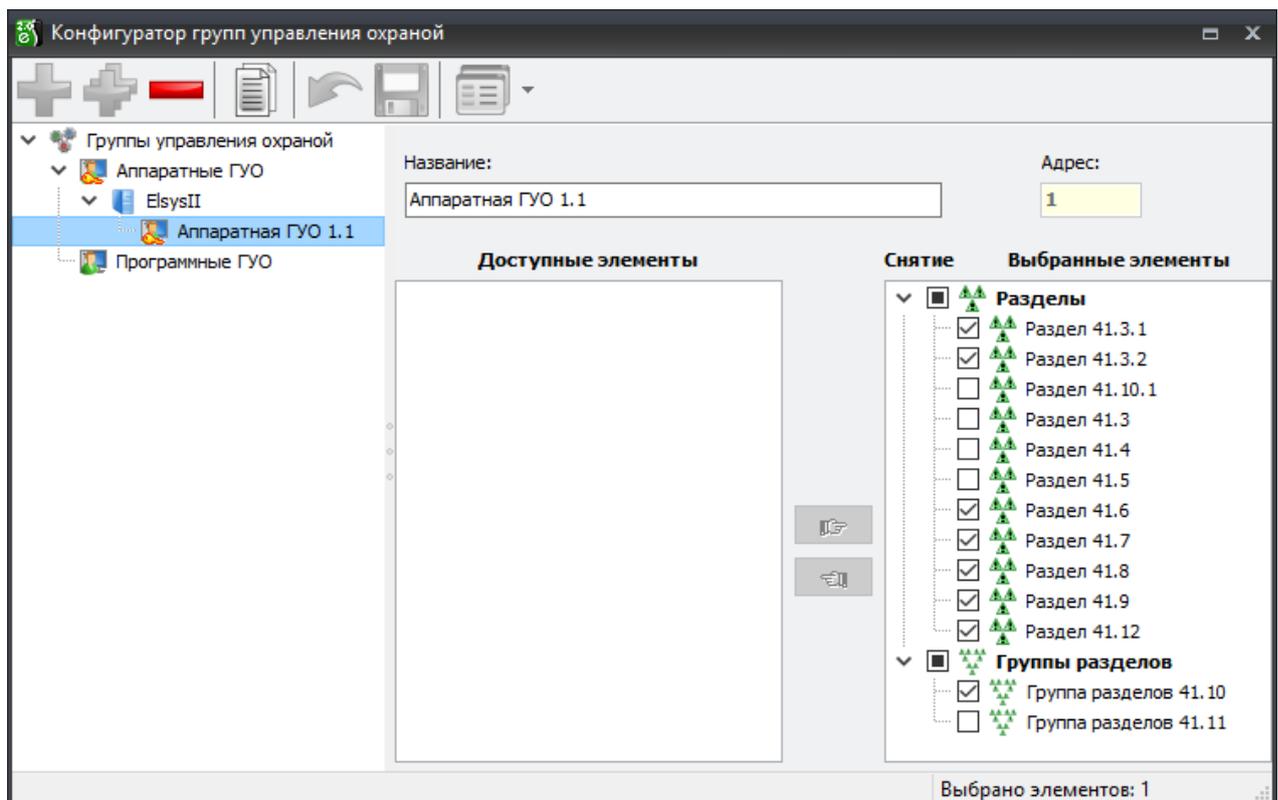


Рисунок 25 – Окно настройки групп управления охраной

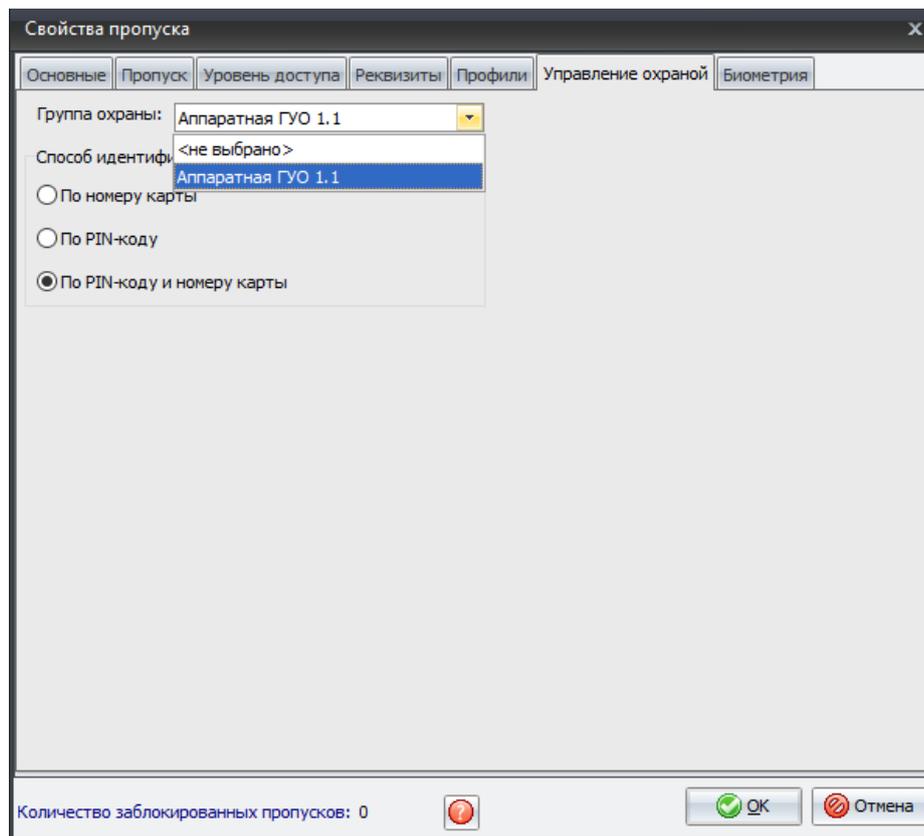


Рисунок 26 – Вкладка «Управление охраной» окна свойств пропуска

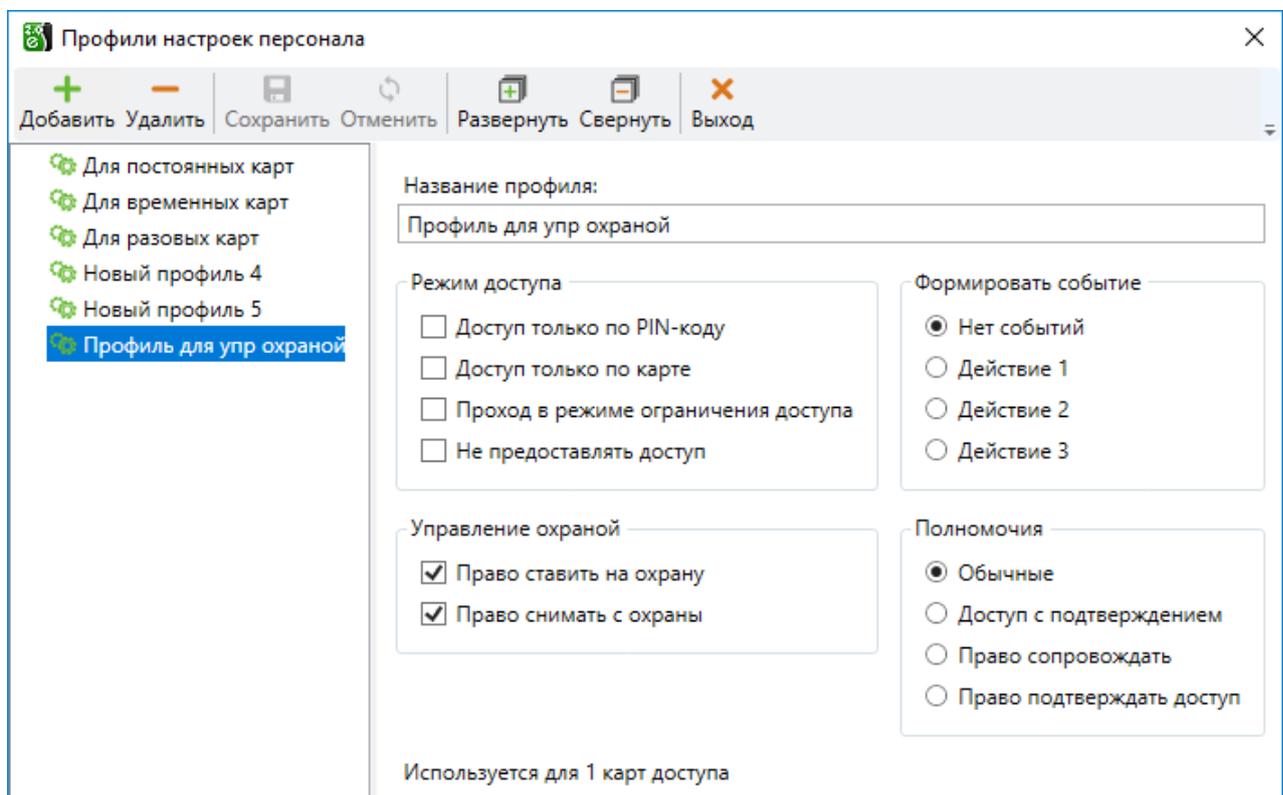


Рисунок 27 – Окно профилей настроек персонала

Следует учитывать, что полномочия по управлению разными локальными разделами в контролерах Elsys-MB и Elsys-NG-xx не разграничиваются. Дополнительно, для возможности управления охраной необходимо, чтобы пользователь СКУД обладал всеми необходимыми правами доступа в точке управления охраной (чтобы считыватель входил в состав уровня доступа, назначенного пользователю). Кроме того, необходимо настроить считыватель таким образом, чтобы обеспечить не только функции управления доступом, но и возможность управления охраной (см. документ «СКУД Elsys. Руководство по настройке»).

#### 4.8 Программы управления выходами

К выходам контроллеров могут быть подключены световые и звуковые оповещатели, линии ПЦН и иные исполнительные устройства, настройка выходов детально описана в документе «СКУД Elsys. Руководство по настройке».

В качестве выходов оповещения могут использоваться выходы охранных контроллеров Elsys-MB-AC, Elsys-AC2 и контроллеров доступа Elsys-MB и Elsys-NG-xx.

**ВНИМАНИЕ! В настройках оборудования и управляющего программного обеспечения необходимо полностью исключить возможность непосредственного управления выходами оповещения, так как это может привести к некорректной работе программ управления выходами.**

Настройка выходов оповещения осуществляется в конфигураторе оборудования СКУД Elsys.

При использовании централизованного режима управления охраной программы управления выходами задаются в настройках охранной подсистемы КСК в окне «Управляющие выходы» (см. Рисунок 28).

Чтобы использовать выход в качестве выхода оповещения централизованной ОС следует добавить выход в список выходов, управляемых КСК, задать для него программу управления и сформировать список разделов, связанных с выходом. Список разделов может включать локальные разделы,

глобальные разделы и группы разделов. Программы управления выходами загружаются в энергонезависимую память ЦКОС при инициализации ОС.

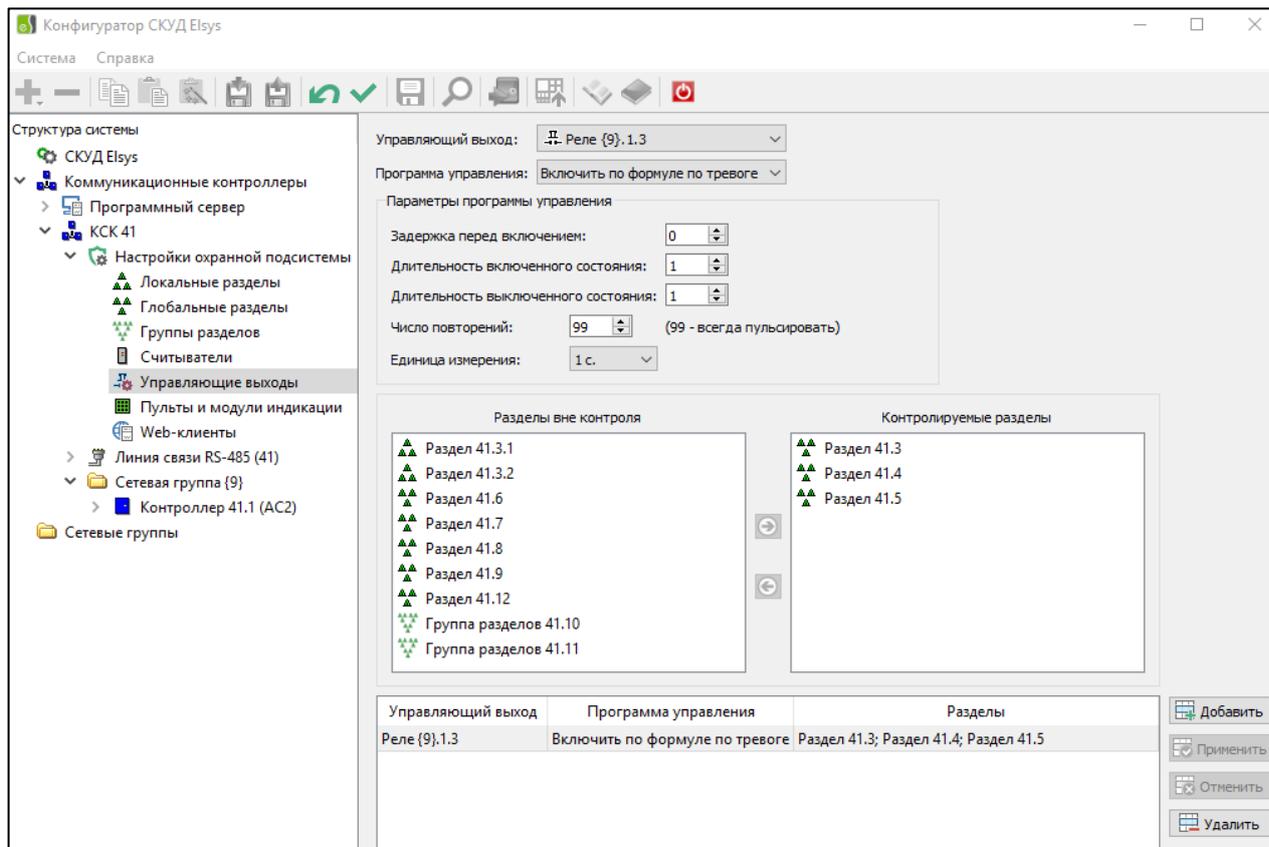


Рисунок 28. Настройка выходов оповещения централизованной ОС

При локальном управлении охраной программы управления выходами задаются в конфигурации контроллеров в узле «Настройка выходов оповещения» (см. Рисунок 29).

В качестве управляющего выхода может быть назначен любой свободный выход контроллера или группа выходов. Для каждого управляющего выхода должна быть задана программа управления и сформирован список ШС, на состояния которых должен реагировать выход. Программы управления выходами, при этом, загружаются в энергонезависимую память контроллеров при инициализации оборудования.

При централизованном управлении охраной программы управления выходами задают режим работы выхода с учётом состояния входящих в него разделов. При локальном управлении программы управления выходами задают режим работы выхода с учётом состояния входящих в него ШС.

В таблице (Таблица 18) приведено описание программ управления ВЫХОДАМИ.

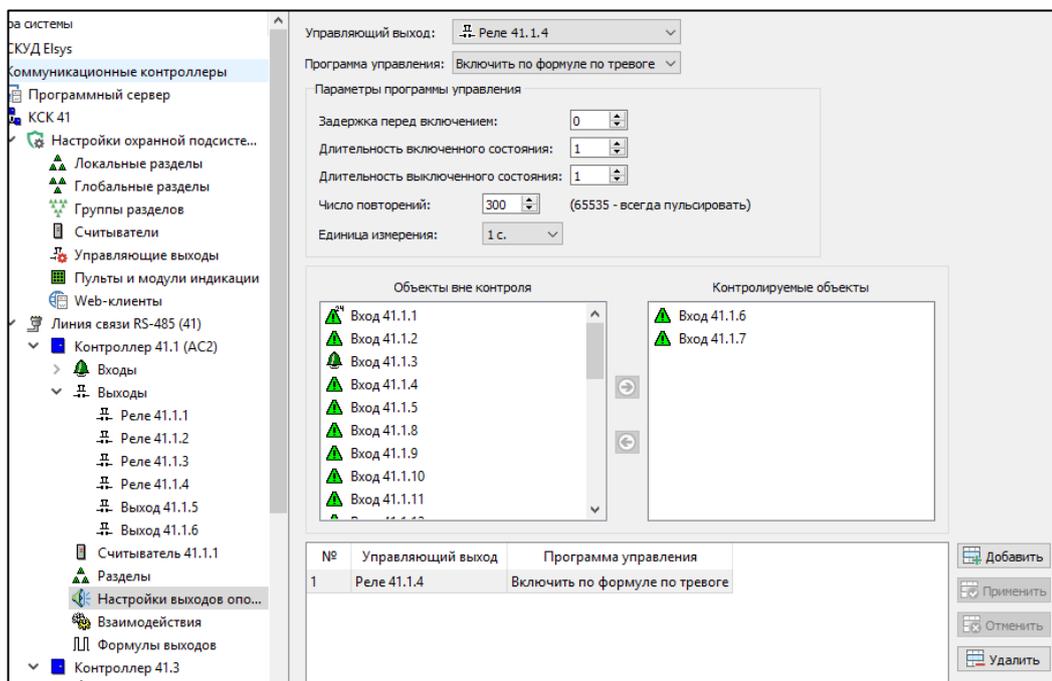


Рисунок 29. Настройка выходов оповещения при локальном управлении охраной

Таблица 18. Программы управления выходами

Программа управления	Описание работы
0 – Нет управления	Управляющий выход выключен
1 – Лампа	<p>Программа, предназначенная для управления световым оповещателем.</p> <p>Если хотя бы один из связанных разделов (ШС) находится в состоянии «Тревога», «Задержка тревоги», «Задержка взятия – неготовность», «Невзятие», «Неисправность», управляющий выход пульсирует с частотой 1 Гц (0,5 с включено, 0,5 с выключено).</p> <p>Если хотя бы один из связанных разделов (ШС) находится в состоянии «На охране» или «Задержка взятия – готовность», и нет ни одного связанного</p>

Программа управления	Описание работы
	<p>раздела (ШС), находящегося в одном из состояний «Тревога», «Задержка тревоги», «Задержка взятия – неготовность», «Невзятие», «Неисправность», управляющий выход находится в состоянии «Включено».</p> <p>Если все разделы (ШС) сняты с охраны и находятся в одном из состояний – «Неготовность» или «Норма – готовность», управляющий выход находится в состоянии «Выключено».</p>
2 – ПЦН	<p>Программа, предназначенная для выдачи извещений на пульт централизованного наблюдения.</p> <p>Если все связанные разделы (ШС) находятся в состоянии «На охране», управляющий выход находится в состоянии «Включено», иначе – в состоянии «Выключено».</p>
3 – Включить, если тревога	<p>Если хотя бы один из связанных разделов (ШС) находится в состоянии «Тревога», управляющий выход находится в состоянии «Включено», иначе – в состоянии «Выключено».</p>
4 – Включить по формуле, если тревога	<p>Если хотя бы один из связанных разделов (ШС) перешёл в состояние «Тревога», управляющий выход начинает работать по программе, задаваемой параметрами «Задержка включения», «Длительность положительной части периода», «Длительность отрицательной части периода», «Число повторений», «Единица измерения».</p> <p>Если ни один из связанных разделов (ШС) не находится в состоянии «Тревога», управляющий выход находится в состоянии «Выключено».</p>
5 – Пожарная лампа	<p>Программа, предназначенная для управления световым оповещателем.</p> <p>Если хотя бы один из связанных разделов (ШС) находится в состоянии «Тревога», «Задержка тревоги», «Задержка взятия – неготовность», «Невзятие», «Неисправность», управляющий выход пульсирует с частотой 1 Гц (0,5 с включено, 0,5 с выключено).</p>

Программа управления	Описание работы
	<p>Если все связанные разделы (ШС) находятся в состоянии «На охране», управляющий выход находится в состоянии «Включено».</p> <p>Если хотя бы один связанный раздел (ШС) снят с охраны, и ни один из связанных разделов не находится в состоянии «Тревога», «Задержка тревоги», «Задержка взятия – неготовность», «Невзятие», «Неисправность», управляющий выход находится в состоянии «Выключено».</p>
<p>Примечание – Для выходов релейных модулей Elsys-AC-RM2, используемых в качестве дополнительных выходов охранных контроллеров Elsys-AC2, при глобальном и при локальном управлении не допускается использовать программу управления «ПЦН», так как релейные выходы этих устройств не обеспечивают необходимое условие для работы тактики «ПЦН» – автоматическое размыкание выхода при обесточивании устройства.</p>	

Для программы управления «Включить по формуле по тревоге» доступна группа настроек «Параметры программы управления», задающая параметры сигнала управления выходом. Допустимые значения параметров формулы выхода приведены в таблице (Таблица 19).

Таблица 19.

Параметры программы управления «Включить по формуле по тревоге»

Параметр	Допустимые значения
Задержка перед включением	0 – 98 с
Длительность включенного состояния	0 – 98 с
Длительность выключенного состояния	0 – 98 с
Число повторений	При локальном управлении: 1 – 65534, 65535 – всегда пульсировать
	При централизованном управлении: 1 – 98 с, 99 – всегда пульсировать
Единица измерения	<ul style="list-style-type: none"> <li>• 0,1 с</li> <li>• 1 с</li> </ul>

Параметр	Допустимые значения
	<ul style="list-style-type: none"><li>• 10 с</li><li>• 1 мин</li><li>• 10 мин</li></ul>

#### 4.9 Совместное использование локального и централизованного управления

В охранной подсистеме СКУД Elsys локальная и централизованная логика управления охранной сигнализацией могут использоваться одновременно.

Любой из входов охранных контроллеров и контроллеров доступа может входить либо в локальный раздел этого контроллера, либо в глобальный раздел, обслуживаемый ЦКОС.

В группы управления охраной, назначаемые пользователям, могут входить как локальные, так и глобальные разделы.

Если группа управления охраной содержит глобальные разделы, то информация о полномочиях по управлению ими и список пользователей, использующих эту группу, будут загружаться в КСК.

Если группа управления охраной содержит локальные разделы, то информация о полномочиях по управлению ими и список пользователей, использующих эту группу, будут загружаться в охранные контроллеры.

Если группа управления охраной содержит глобальные и локальные разделы, то в КСК и охранные контроллеры будут загружаться необходимые для работы подмножества групп управления охраной и соответствующие им списки пользователей.

Если локальный раздел добавлен в список разделов, управляемых централизованно, то в этом случае полномочия по управлению этим разделом и списки пользователей загружаются в память центрального контроллера, а охранный контроллер (Elsys-AC2, Elsys-MB-AC) или контроллер доступа Elsys-MB, Elsys-NG-xx обеспечивает логику формирования интегрального состояния этого раздела.

Если считыватель охранного контроллера оснащён клавиатурой, то при управлении режимами охраны кодовая комбинация, введённая с клавиатуры,

выбирает раздел (локальный или глобальный), для которого запрашиваются полномочия для управления. Если считыватель не оснащён клавиатурой, то сначала проверяются полномочия для локального управления охраной, и, если они отсутствуют, выполняется запрос полномочий у ЦКОС (КСК Elsys-MB-Net II или Elsys-NG-Net II).

## 5 Дополнительные сведения по настройке охранной подсистемы

### 5.1 Начальная настройка КСК и охранных контроллеров

КСК, охранные контроллеры, клавиатуры Elsys-CP2 и другое оборудование СКУД Elsys поставляются с настройками по умолчанию. Для начальной настройки этих устройств следует использовать окно конфигуратора «Поиск устройств».

Для поиска КСК и задания сетевых настроек следует использовать вкладку «Поиск КСК» (см. Рисунок 30).

Для поиска и начальной настройки контроллеров, подключаемых через Ethernet, следует использовать вкладку «Поиск контроллеров в сетевых группах» (см. Рисунок 31).

**ВНИМАНИЕ! Поиск устройств в сети Ethernet возможен лишь в случае, если разрешено прохождение широковещательных пакетов между сервером интеграции и оборудованием. Если конфигурация сети не позволяет выполнить поиск, следует осуществлять начальную настройку с ближайших сетевых рабочих мест, либо использовать опцию «Искать через управляющий КСК».**

Для поиска и начальной настройки контроллеров, подключаемых в линию RS-485, следует использовать вкладку «Поиск контроллеров в линиях RS-485» (см. Рисунок 32). Если в линию RS-485 подключено несколько устройств, имеющих одинаковый адрес (например, с настройками по умолчанию), следует выполнять поиск с включенной опцией «Поиск по серийному номеру». Чтобы различать однотипные устройства при поиске, рекомендуется использовать информацию о состоянии корпуса («Открыт»/«Закрыт») – например, открыв дверцу корпуса у одного из устройств.

После выполнения поиска и задания сетевых настроек устройство может быть добавлено в базу данных конфигурирования кнопкой «Добавить в базу».

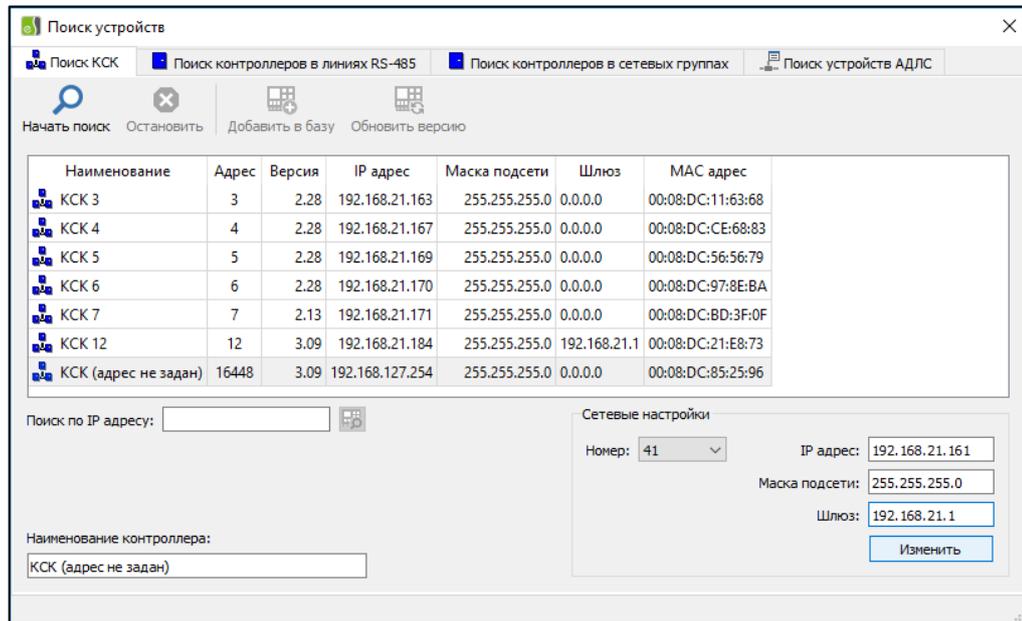


Рисунок 30. Поиск КСК

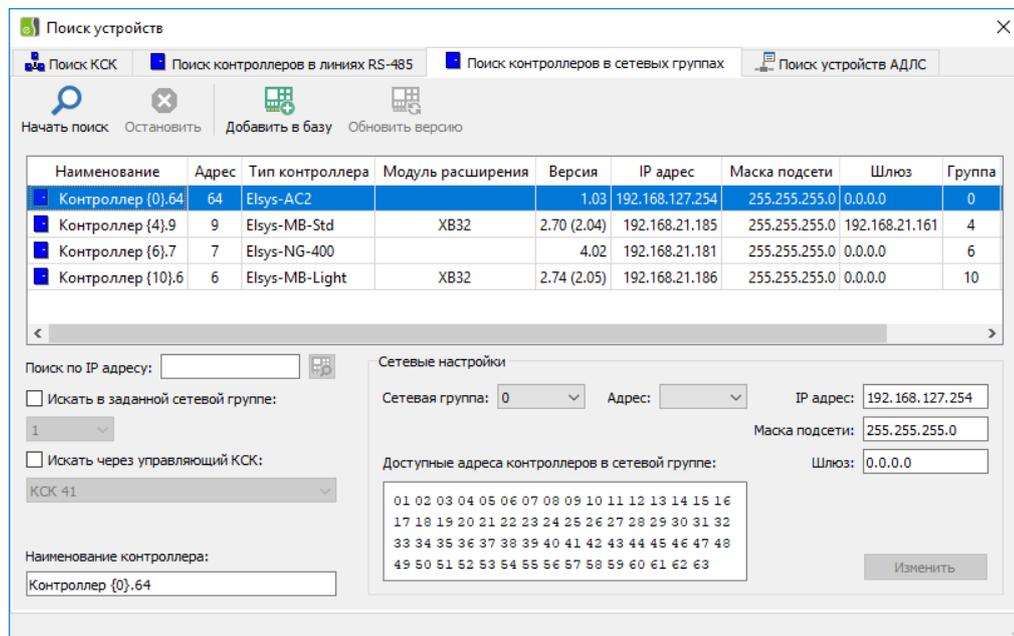


Рисунок 31. Поиск контроллеров в сетевых группах

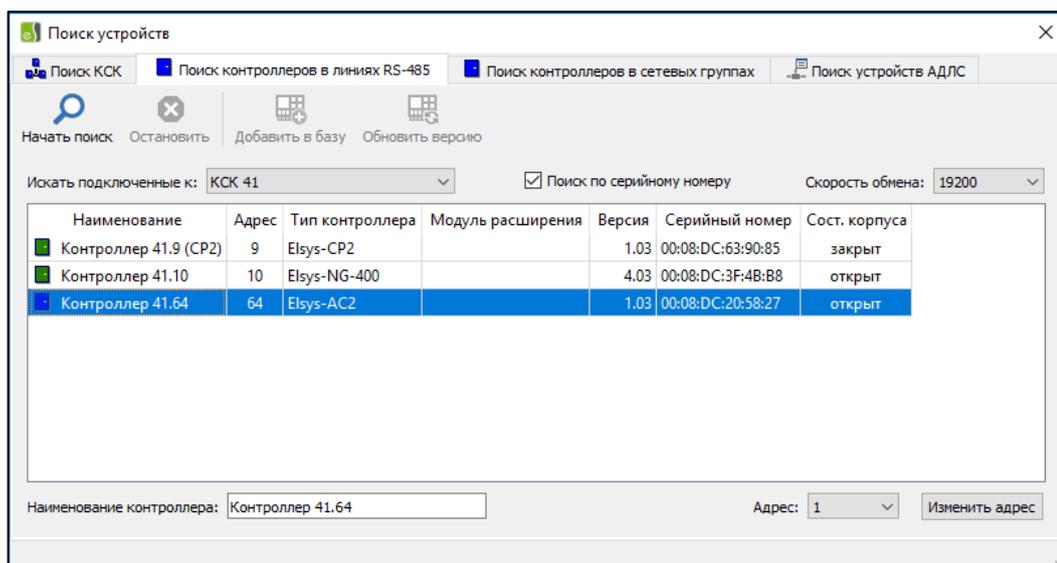


Рисунок 32. Поиск контроллеров в линиях RS-485

## 5.2 Начальная настройка устройств адресной двухпроводной линии

Для выполнения поиска устройств АДЛС и назначения им адресов в охранных контроллерах Elsys-AC2 предусмотрен специальный сервисный режим, который включается в конфигураторе на вкладке «Поиск устройств АДЛС» (см. Рисунок 33).

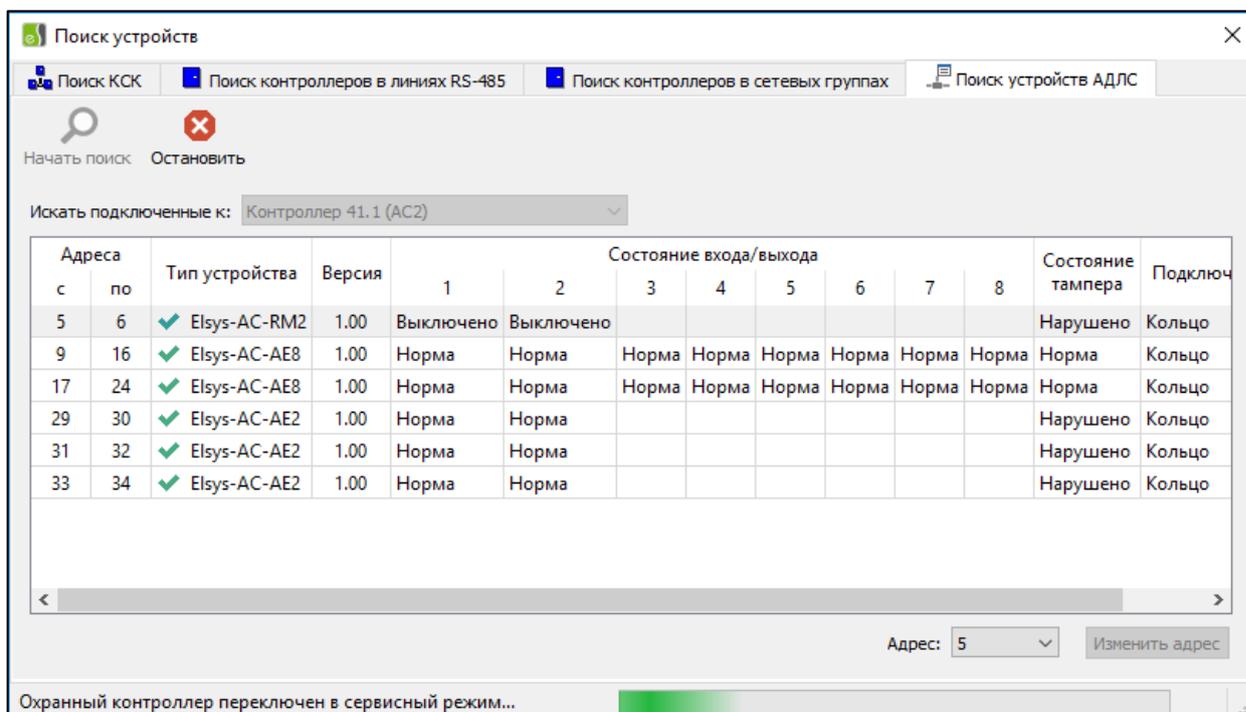


Рисунок 33. Поиск устройств АДЛС

Для включения этого режима необходимо выбрать в списке «Искать подключенные к:» один из охранных контроллеров и нажать кнопку «Начать поиск».

Контроллер, находящийся в этом режиме, приостанавливает дежурный опрос расширителей и выполняет непрерывное сканирование устройств АДЛС во всём диапазоне адресов (1 – 255), обновляя текущую информацию. В процессе отображения информации, если ещё не все данные получены от оборудования, конфигуратор может временно отображать неполную информацию (например, сообщать, что тип расширителя или его версия неизвестны).

Если необходимо сменить адрес расширителя, следует, не прекращая режим поиска, выбрать в таблице нужный расширитель, затем, установив новое значение адреса, нажать кнопку «Изменить адрес».

Подробно поиск устройств АДЛС описан в документе «Конфигуратор СКУД Elsys. Руководство пользователя».

При эксплуатации системы все устройства АДЛС должны иметь уникальные адреса. Однако, при начальной настройке после монтажа оборудования возможна ситуация, при которой расширители имеют совпадающие адреса, соответствующие заводским установкам (для Elsys-AC-AE2 и Elsys-AC-RM2 – стартовый адрес 254, для Elsys-AC-AE8 – 248, для адресных извещателей Elsys-AC-IRV, Elsys-AC-GB, Elsys-AC-IRF, Elsys-AC-MC – 255). В такой ситуации следует использовать функцию присвоения временного адреса конкретному устройству АДЛС. Числовое значение временного адреса – 501.

Для установки временного адреса (в устройствах, кроме извещателя Elsys-AC-MC) следует:

- открыть крышку устройства, чтобы тампер перешёл в состояние «нарушено», и подождать 10 секунд;
- выполнить серию из четырёх нажатий на тампер (короткое, длинное, короткое, длинное). Длительность короткого нажатия не более 0,5 с, а длительность длинного нажатия – от 0,5 до 1 с, длительность паузы между нажатиями – не более 1 с. Если тампер выполнен в виде

магнитоконтактного устройства, следует соответствующим образом выполнять поднесение магнита;

- убедиться, что успешное окончание серии нажатий подтверждено кратковременным включением светодиода в непрерывном или мигающем режиме (в зависимости от типа устройства);
- в течение 5 минут выполнить смену временного адреса на постоянный.

Для установки временного адреса в извещателе Elsys-АС-МС следует:

- замкнуть контакты металлическим предметом на 2 секунды (см. Рисунок 34);
- в течение 5 минут выполнить смену временного адреса на постоянный.

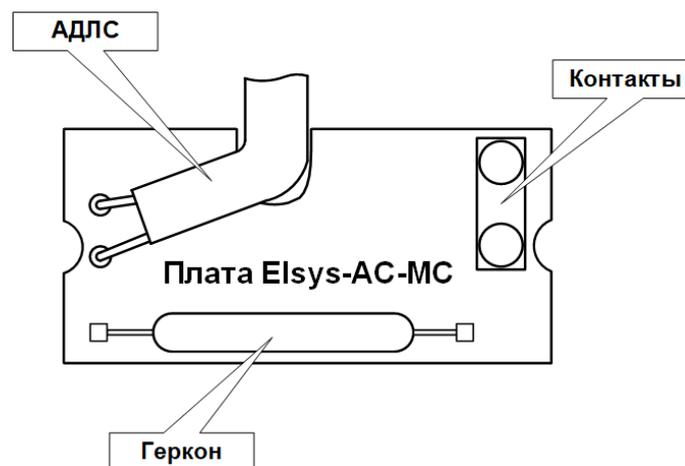


Рисунок 34 – Установка временного адреса в Elsys-АС-МС

### 5.3 Загрузка конфигурации системы в оборудование (инициализация оборудования)

#### 5.3.1 *Инициализация аппаратных настроек*

После внесения любых изменений в конфигурацию оборудования (свойства устройств, состав разделов, и т. д.) необходимо выполнить полную инициализацию оборудования, в настройках которого были сделаны изменения,

для чего следует вызвать окно конфигуратора «Управление сервером интеграции», вид которого приведён на рисунке (Рисунок 35).

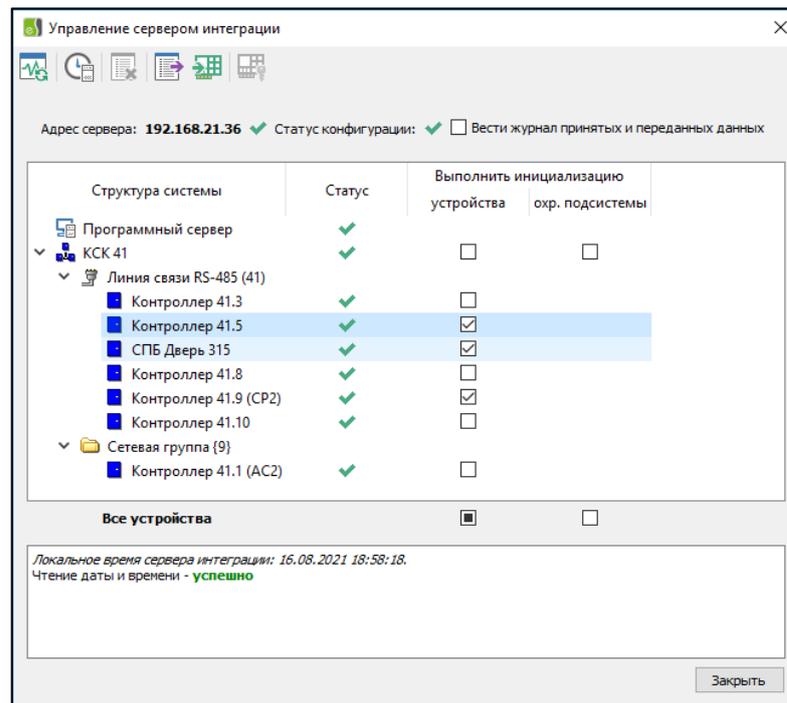
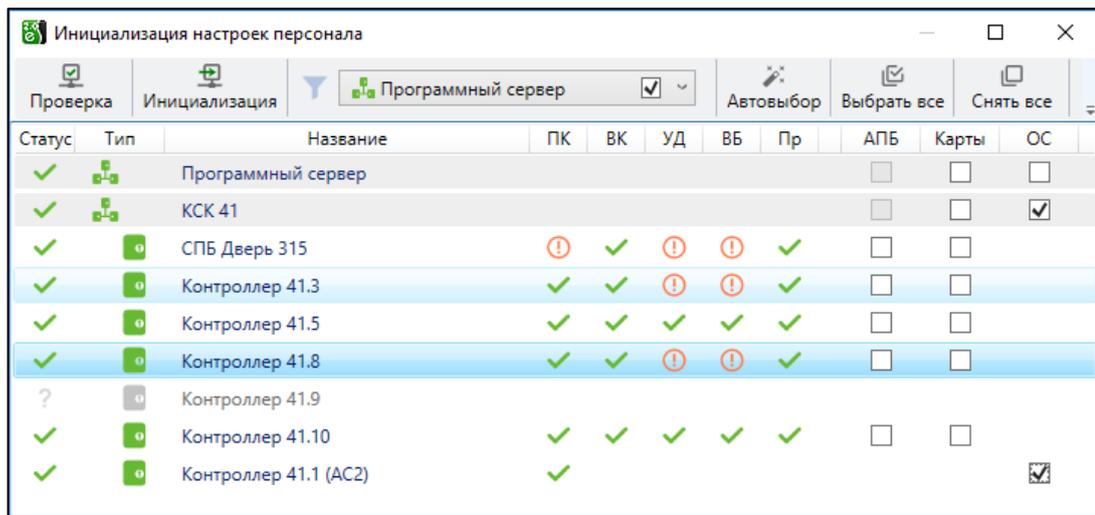


Рисунок 35 – Окно управления сервером интеграции

### 5.3.2 Инициализация настроек персонала

При дальнейшей работе системы все изменения списка пользователей охранной сигнализации и наборов их полномочий будут загружаться в оборудование автоматически. Повторная инициализация настроек персонала может потребоваться в случае длительного отсутствия связи с оборудованием, а также в случае, если в конфигурацию оборудования были внесены изменения и выполнялась инициализация оборудования.

Инициализация настроек персонала выполняется из клиентского программного обеспечения. Вид окна инициализации приведён на рисунке (Рисунок 36).



Статус	Тип	Название	ПК	ВК	УД	ВБ	Пр	АПБ	Карты	ОС
✓	Программный сервер	Программный сервер						<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
✓	КСК 41	КСК 41						<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
✓	СПБ Дверь 315	СПБ Дверь 315	⚠	✓	⚠	⚠	✓	<input type="checkbox"/>	<input type="checkbox"/>	
✓	Контроллер 41.3	Контроллер 41.3	✓	✓	⚠	⚠	✓	<input type="checkbox"/>	<input type="checkbox"/>	
✓	Контроллер 41.5	Контроллер 41.5	✓	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	
✓	Контроллер 41.8	Контроллер 41.8	✓	✓	⚠	⚠	✓	<input type="checkbox"/>	<input type="checkbox"/>	
?	Контроллер 41.9	Контроллер 41.9								
✓	Контроллер 41.10	Контроллер 41.10	✓	✓	✓	✓	✓	<input type="checkbox"/>	<input type="checkbox"/>	
✓	Контроллер 41.1 (AC2)	Контроллер 41.1 (AC2)	✓							<input checked="" type="checkbox"/>

Рисунок 36 – Окно инициализации настроек персонала

На приведённом рисунке в колонке «ОС» (охранная сигнализация) отмечены устройства, в которые будет загружена информация о полномочиях пользователей охранной подсистемы.