Группа компаний «ТвинПро»

ООО «ЕС-пром»

Система контроля и управления доступом большой ёмкости с функциями охранной сигнализации Elsys

РУКОВОДСТВО ПО НАСТРОЙКЕ

ЕСЛА.425723.400 ИС

2024

СОДЕРЖАНИЕ

Настоящее руководство предназначено для изучения принципа работы, ознакомления с порядком настройки и эксплуатации системы контроля и управления доступом большой ёмкости с функциями охранной сигнализации Elsys (в дальнейшем – система).

В настоящем руководстве приняты следующие сокращения и обозначения:

СКУД – система контроля и управления доступом;

КД – контроллер доступа;

УПУ – устройства преграждающие управляемые, к которым относятся двери, турникеты, шлагбаумы, калитки и т. п.;

ПО – программное обеспечение;

АРМ – автоматизированное рабочее место;

ПК – персональный компьютер;

УИ – устройства исполнительные;

УС – устройство считывания, считыватель;

ШС – шлейф сигнализации;

АДЛС – адресная двухпроводная линия связи;

PIN-код – дополнительный идентификационный признак пользователя, вводимый с клавиатуры.

Версия настоящего документа – 1.01 (10.2024).

1 Описание и работа системы

1.1 Назначение и состав системы

Система предназначена для организации автоматического контроля и управления доступом на объектах различного масштаба – на проходных зданий и учреждений, в помещениях особой важности, авторизации управления различными элементами системы безопасности (например, автоматическими воротами, шлагбаумами, лифтами и т. п.), автоматического управления исполнительными механизмами по заданным событиям и временным расписаниям. Система обеспечивает поддержку функций охранной

сигнализации, а также интеграцию с системами охранной и охранно-пожарной сигнализации и системами видеоконтроля как на релейном, так и на системном уровне.

В состав СКУД Elsys входят аппаратные средства:

- контроллеры доступа Elsys-MB вариантов исполнения Pro, Std, Light, Pro4 с функциями охранной сигнализации;
- контроллеры доступа Elsys-MB-SM, являющиеся функционально упрощёнными моделями контроллеров Elsys-MB;
- контроллеры доступа Elsys-NG-200, Elsys-NG-800 и Elsys-NG-1000 (далее – Elsys-NG-xx) с функциями охранной сигнализации;
- контроллеры доступа серии ЛКД-КС-2000;
- релейные модули Elsys-RM-16C;
- модули Elsys-IO/MB (содержат 16 выходов типа «открытый коллектор»);
- преобразователи интерфейсов Elsys-RC-232/485 и Elsys-CU-USB-232/485, предназначенные для сопряжения сети контроллеров с персональным компьютером;
- интерфейсные модули Elsys-IP, предназначенные для подключения контроллеров линейки Elsys-MB (кроме Elsys-MB-SM) в сеть Ethernet;
- коммуникационные сетевые контроллеры Elsys-MB-Net, Elsys-MB-Net II, Elsys-NG-Net II, предназначенные для объединения контроллеров в единую систему через сеть Ethernet;
- 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-MC, 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 состояний охранных разделов;

– считыватели линейки Elsys-SW производства группы компаний «ТвинПро» (либо аналогичные иных производителей).

К программным средствам СКУД Elsys относятся:

– сервер интеграции, выполненный в виде программного сервиса;
– конфигуратор СКУД Elsys;
– клиентское программное обеспечение.

Для настройки системы пользователь должен ознакомиться с эксплуатационной документацией на используемое оборудование и клиентское программное обеспечение, а также с документами «Программный сервис Elsys-SDK II. Руководство администратора», «Конфигуратор СКУД Elsys. Руководство пользователя» и «ТСОС Elsys. Руководство по эксплуатации».

В состав клиентского программного обеспечения 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.

Функциональная схема, описывающая взаимодействие программных и аппаратных средств СКУД Elsys, приведена на рисунке (Рисунок 1).

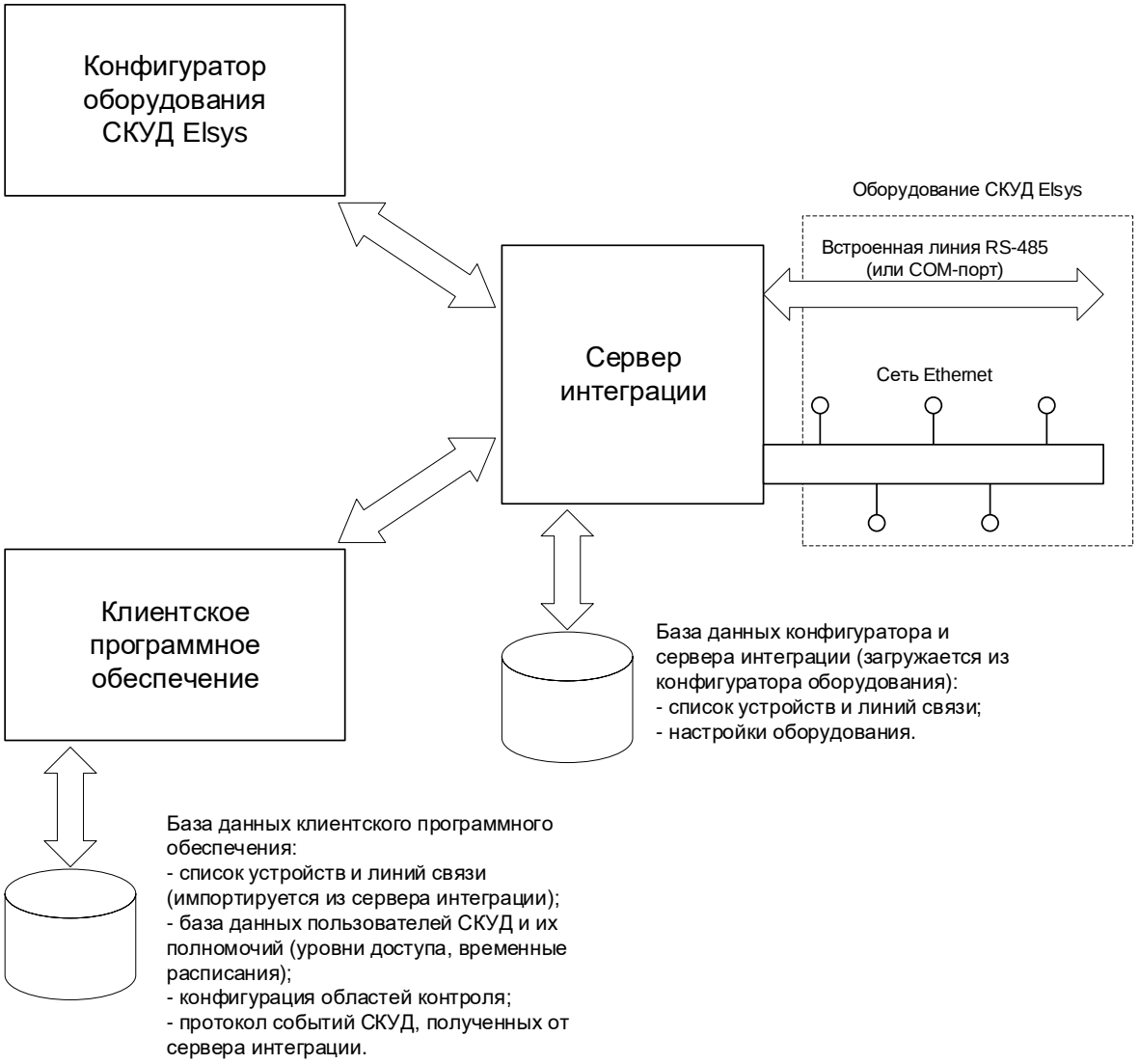

Рисунок 1. Взаимодействие программных и аппаратных средств

1.2 Основные термины и понятия

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.

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

Линия связи может быть либо физической линией связи RS-485, либо сетевой группой, представляющей собой логическое объединение контроллеров, поддерживающих IP-протоколы и физически подключаемых по

интерфейсу Ethernet. Адресная ёмкость линии связи СКУД Elsys – 63 контроллера.

Коммуникационный сетевой контроллер (КСК) выполняет:

- опрос до 63 контроллеров, подключенных в линию связи RS-485;
- опрос до 63 контроллеров, включенных в сеть Ethernet и объединённых в сетевую группу;
- обмен данными в едином информационном пространстве с контроллерами в линии RS-485, сетевой группе и с другими КСК для организации межконтроллерных взаимодействий и глобального контроля последовательности прохода.

Контроллер – адресное устройство СКУД Elsys, включаемое в линию связи RS-485 или сетевую группу.

Устройство – объект системы, описывающий элемент или набор элементов физического оборудования СКУД Elsys или их свойства.

К устройствам относятся:

- КСК;
- линии связи;
- контроллеры;
- точки доступа (двери, турникеты, ворота);
- считыватели;
- охранные зоны и входы контроллеров;
- охранные разделы и группы разделов;
- выходы и группы выходов.

1.3 Технические характеристики

1.3.1 Функциональные возможности системы

Система обеспечивает следующие функциональные возможности:

- настройку с помощью программного обеспечения и загрузку в энергонезависимую память оборудования следующих данных:
  1) идентификационные признаки пользователей системы с назначенными индивидуальными параметрами (в том числе срок действия идентификатора);

2) временные блоки, состоящие из нескольких временных интервалов;
3) уровни доступа, каждый из которых является совокупностью разрешённых точек доступа и назначенных для них временных блоков. Каждому пользователю системы назначается один из заранее настроенных уровней доступа;
4) праздничные дни (с возможностью назначения в эти дни особых режимов доступа);
5) настройки контроллера, обеспечивающие работу подключаемого к ним оборудования (УПУ, УС, УИ и т.п.) в нужных режимах;

– перечисленные ниже функции контроля и управления УПУ в точках доступа:

1) формирование сигналов открывания УПУ включением назначенного реле или слаботочного выхода, включенного в цепь УИ, при считывании зарегистрированного в памяти системы идентификационного признака и принятия решения о предоставлении доступа;

2) формирование сигналов для автоматического запирания УПУ после совершения фактического прохода;

3) формирование сигналов, запирающих УПУ по истечении времени, отведённого на совершение прохода;

4) настройку времени включения УПУ, задержки включения, и времени, в течение которого разрешается доступ;

5) регистрацию фактического прохода по срабатыванию датчика прохода;

– регистрацию и накопление событий (с ведением даты и времени) в энергонезависимой памяти контроллеров и КСК. При установлении связи все события, накопленные в памяти контроллеров и КСК, передаются в компьютер для обработки;
– использование клавиатур, встраиваемых в считыватели, для ввода дополнительного идентификационного признака (PIN-код);
– ввод специального идентификационного признака для открывания под принуждением;
– глобальный контроль последовательности прохода (защита от повторного использования идентификатора для прохода в одном направлении),

сохраняющий свою полную функциональность при отсутствии компьютера на линии связи;

- организацию доступа по правилу двух и более лиц;
- организацию доступа с подтверждением дежурного оператора;
- управление устройствами, подключенными к контроллерам доступа, по временным расписаниям;
- возможность программирования логики работы контроллеров;
- сохранение всех основных функций при нарушении связи с сервером интеграции или клиентским программным обеспечением;
- автоматический контроль исправности устройств (самотестирование) и линии связи.

Технические средства охранной сигнализации, входящие в состав СКУД 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.

Программные средства, входящие в состав системы, обеспечивают:

- регистрацию и протоколирование в базе данных текущих и тревожных событий, передаваемых контроллерами, с приоритетным отображением на рабочем месте дежурного оператора событий, происходящих в реальном времени;

- отображение и регистрацию нарушения и восстановления связи с приборами;
- отображение на экране персонального компьютера плана объекта и/или помещений объекта с указанием расположения средств контроля доступа, охранно-пожарной сигнализации и видеоконтроля в виде пиктограмм и графическое отображение тревожных состояний в контрольных точках на плане;
- интерактивное управление средствами (в том числе режимами работы точек доступа) по изображению плана объекта на мониторе персонального компьютера;
- ведение базы данных пользователей системы, включая фотографии сотрудников;
- контроль над перемещением пользователей системы и их поиск по месту последнего предъявления карты;
- фотоидентификацию пользователей;
- настройку параметров отображения событий и полномочий для лиц обслуживающего персонала системы;
- парольную защиту при входе в систему;
- формирование отчётов по событиям, в том числе учёт фактического рабочего времени сотрудников;
- интеграцию на системном уровне (с помощью управляющего программного обеспечения) с системами видеонаблюдения, системами охранно-пожарной сигнализации и системами контроля и управления доступом других производителей.

1.3.2 Основные технические характеристики СКУД Elsys

Таблица 1.

Технические характеристики системы

Наименование параметра	**Значение**
Максимальное количество контроллеров в системе	32067
Максимальное количество точек доступа в системе	

Наименование параметра	Значение
Двусторонних Односторонних	32067 64124
Длина значащей части номера карты	3 байта, 6 байт или 8 байт (определяется общими настройками системы)
Контроль последовательности прохода (antipassback)	глобальный аппаратный (в рамках всей системы); глобальный программный (в рамках всей системы); локальный (в пределах одного контроллера).
Максимальное количество зон доступа в системе	4095
Максимальное количество зон доступа, обслуживаемых контроллерами из нескольких линий связи	63
Максимальное количество уровней доступа в системе	16382
Максимальное количество временных блоков в системе	16382
Максимальное количество праздничных дней	32
Максимальное количество пользователей системы	Определяется исполнением используемых контроллеров и их количеством
Режимы прохода	Только карта Только PIN-код PIN-код + карта Вход под принуждением Две карты Три карты Карта + кнопка подтверждения Карта + карта подтверждения Свободный выход по кнопке
Интерфейс считывателей	Wiegand (Wiegand-26, Wiegand-32, Wiegand-33, Wiegand-34, Wiegand-36, Wiegand-37, Wiegand-40, Wiegand-42, Wiegand-44, Wiegand-48, Wiegand-56, Wiegand-58, Wiegand-64, Wiegand-66); ES-Wiegand (Wiegand-128 защищённый); Touch Memory; ESDP.
Коммуникационные интерфейсы	Ethernet 10/100 Mbps Двухпроводный RS-485
Скорость обмена информацией по линии связи RS-485, бит/с	4800, 9600, 19200, 38400, 57600, 115200
Максимальное количество	63

Наименование параметра	Значение
контроллеров в линии связи RS-485 или сетевой группе	
Максимальное количество КСК	254
Максимальное количество сетевых групп	254
Максимальное количество линий связи RS-485, непосредственно подключаемых к ПК через преобразователь интерфейса	1
Максимальное количество устройств в системе (независимо от количества линий связи и контроллеров в системе)	1000000

1.3.3 Основные технические характеристики контроллеров доступа

Основные технические характеристики контроллеров доступа приведены в таблице (Таблица 2).

Таблица 2.

Основные технические характеристики контроллеров доступа

Наименование параметра	Тип контроллера							
	Elsys-MB				Elsys-MB-SM	Elsys-NG-200	Elsys-NG-800	Elsys-NG-1000
	Pro	Std	Light	Pro4				
Количество пользователей[1)]	81000 (162000)				4096	75000	100000 (400000)	400000
Количество событий в энергонезависимой памяти[1)]	61000 (122000)				4096	250000	500000	700000
Количество уровней доступа[1)]	1800				240	16382	16382	16382
Количество временных блоков[1)]	1800				240	16382	16382	16382
Количество временных интервалов[1)]	1800				240	64000	64000	64000
Длина значащей части номера карты	3 байта, 6 байт				3 байта	3 байта, 6 байт	3 байта, 6 байт	3 байта, 6 байт, 8 байт
Поддержка временных пропусков	+				–	+		

Наименование параметра	**Тип контроллера**							
	Elsys-MB				Elsys-MB-SM	Elsys-NG-200	Elsys-NG-800	Elsys-NG-1000
	Pro	Std	Light	Pro4				
Интерфейс линии связи с КСК или сервером оборудования	RS-485 Ethernet[2)]				RS-485	RS-485 Ethernet		
Поддержка защищённых сетевых протоколов 802.1x, EAP-TLS, TLS v 1.2, TLS v 1.3, mTLS v 1.2, mTLS v 1.3	–				–	–	–	+
Поддержка протокола DHCP	–				–	–	–	+
Количество односторонних точек доступа	2	2	2	4	2	2	4	4
Количество двусторонних точек доступа	1	1	1	2	1	1	2	2
Поддерживаемые типы точек доступа	дверь турникет ворота				дверь	дверь турникет ворота		
Количество считывателей	2	2	2	4	2	2	4	4
Глобальный аппаратный antipassback[3)]	+	+	+	+	+	+	+	+
Глобальный программный аппаратный antipassback[4)]	+	+	+	+	–	+	+	+
Локальный антипассбэк[3)]	+	+	+	+	+	+	+	+
Количество встроенных входов для подключения шлейфов сигнализации	8	4	2	8	–	8	8	8
Количество охранных разделов	8	4	2	8	–	8	8	8
Возможность программирования логики работы	+				–	+	+	+

Примечания:

1 Приведены одновременно достигаемые максимальные значения количества пользователей и событий. Для контроллеров Elsys-MB характеристики приведены при условии установленного модуля расширения памяти Elsys-XB64 и размере номера карты 3 байта. Для контроллеров Elsys-MB (кроме Elsys-MB-SM) и Elsys-NG-800 количество карт или событий может быть увеличено (до значений, приведённых в

Наименование параметра	**Тип контроллера**							
	Elsys-MB				Elsys-MB-SM	Elsys-NG-200	Elsys-NG-800	Elsys-NG-1000
	Pro	Std	Light	Pro4				
скобках) за счёт уменьшения, соответственно, количества событий или карт. 2 Для подключения в сеть Ethernet контроллеры Elsys-MB должны быть оснащены интерфейсным модулем Elsys-IP и модулем расширения памяти Elsys-XB. 3 Для контроллеров Elsys-MB-SM antipassback доступен при количестве пользователей не более 150. 4 Для поддержки программного antipassback-а необходимо обновить прошивку контроллеров до актуальной версии (подробнее – ниже).								

1.3.4 Основные технические характеристики охранных контроллеров

Основные технические характеристики охранных контроллеров приведены в таблице (Таблица 3).

Таблица 3.

Основные технические характеристики охранных контроллеров

Наименование параметра	**Тип контроллера**	
	Elsys-MB-AC	**Elsys-AC2**
Количество встроенных входов для подключения шлейфов сигнализации	8	8
Количество встроенных релейных выходов	2	4
Количество считывателей	1	1
Количество входов АДЛС	–	247
Количество выходов АДЛС	–	60
Адресная ёмкость АДЛС	–	247
Количество локальных охранных разделов	8	255
Количество пользователей	1024	64000
Максимальное количество событий в энергонезависимой памяти	2048	16000
Количество групп управления охраной	1024	64000
Интерфейс линии связи с КСК или сервером оборудования	RS-485	RS-485 Ethernet
Адресная двухпроводная линия связи	–	+
Диапазон допустимых напряжений на входах, В	0 – 5	0 – 11,5

Номинальное значение оконечного резистора для охранного ШС, кОм	2	2
Номинальное значение оконечного резистора для ШС устройств АДЛС, кОм	–	10

1.3.5 Основные технические характеристики коммуникационных сетевых контроллеров

Таблица 4.

Основные технические характеристики КСК

Наименование параметра	**Тип КСК**		
	Elsys-MB-Net	**Elsys-MB-Net II**	**Elsys-NG-Net II**
Интерфейс связи с сервером интеграции	Ethernet 10/100 Mbps		
Интерфейс связи с контроллерами	Ethernet 10/100 Mbps*) Двухпроводный RS-485		
Количество разъёмов Ethernet (RJ-45)	1	2 (встроенный сетевой коммутатор)	
Поддержка защищённых сетевых протоколов 802.1x, EAP-TLS, TLS v 1.2, TLS v 1.3, mTLS v 1.2, mTLS v 1.3	–	–	+
Поддержка протокола DHCP	–	–	+
Количество охранных зон, обслуживаемых одним КСК	–	4096	
Количество разделов	–	4096	
Количество групп разделов	–	2048	
Количество программируемых выходов	–	512	
Количество пользователей охранной сигнализации	–	64000	
Количество групп управления охраной	–	64000	
Примечание – При использовании КСК Elsys-MB-Net для опроса контроллеров сетевой группы недоступно его использование для обмена информацией между КСК.			

1.4 Описание работы СКУД Elsys

1.4.1 Общие сведения

Структурная схема системы приведена на рисунке (Рисунок 2).

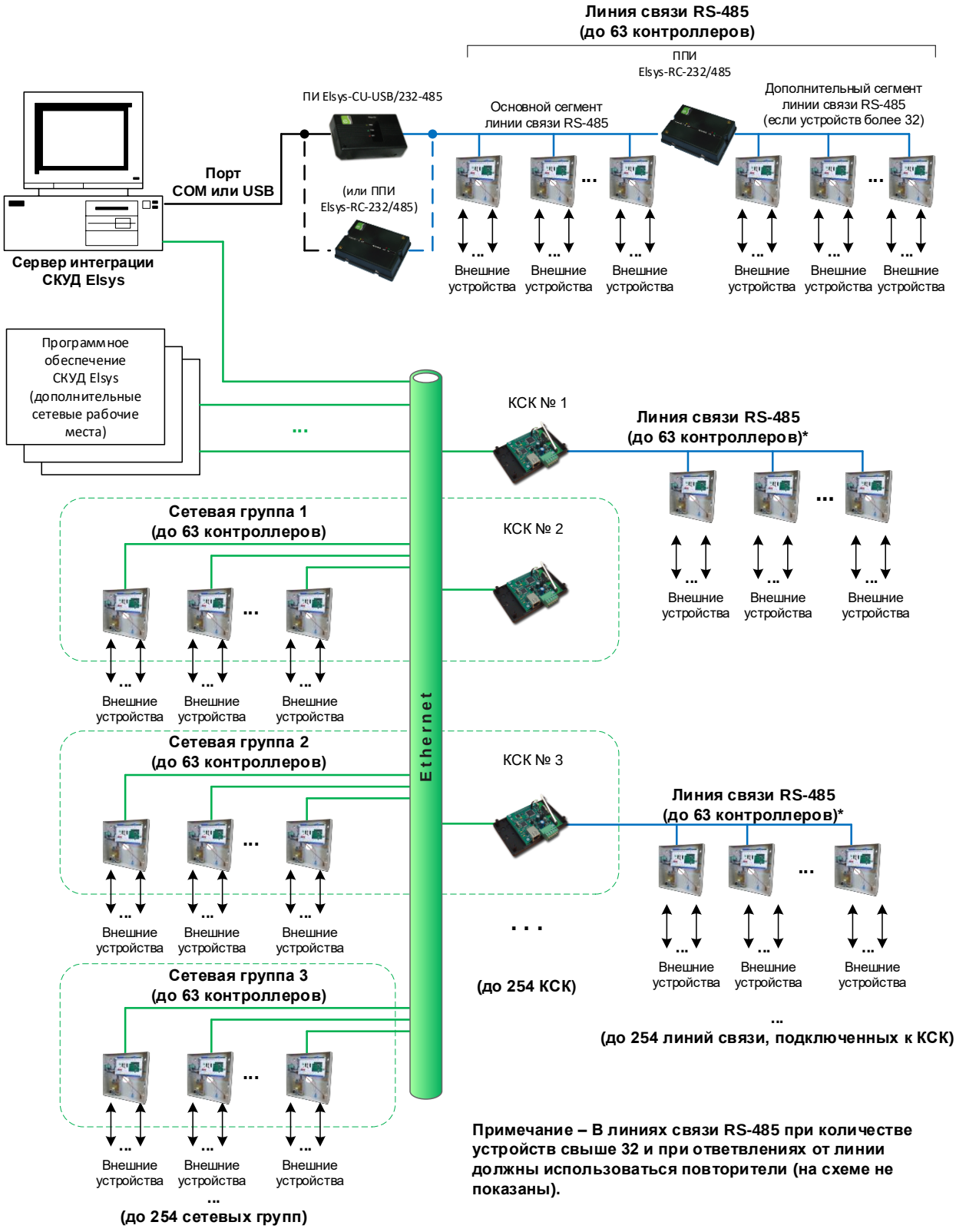

Рисунок 2. Структурная схема СКУД Elsys

Аппаратную основу системы составляют контроллеры доступа и охранные контроллеры, к которым подключаются устройства ввода идентификационных признаков (считыватели и клавиатуры), устройства формирования извещений о внешних событиях (кнопки, реле, контактные и токопотребляющие охранные извещатели и т. п.) и исполнительные устройства (турникеты, дверные электромагнитные и электромеханические замки, приводы ворот, сирены и т.п.).

Контроллеры осуществляют приём информационных посылок от считывателей, непрерывный анализ сигналов, поступающих на входные линии, команд и сообщений, передаваемых ПК и другими контроллерам, и, в соответствии с параметрами, хранящимися в энергонезависимой памяти, управляют исполнительными устройствами.

1.4.2 Протоколирование событий

Все события, регистрируемые контроллерами и КСК, записываются в их энергонезависимую память (буфер событий). Если компьютер участвует в информационном обмене, контроллеры передают все события в реальном времени по мере их поступления. При потере связи с компьютером события накапливаются в буфере событий. Если количество накопленных событий превысит ёмкость буфера событий, самые старые события замещаются вновь поступившими. После восстановления связи с компьютером все события, накопленные в буфере, передаются в хронологическом порядке. При этом новые события, зарегистрированные после восстановления связи, передаются в приоритетном порядке.

Контроллеры и КСК передают в управляющее программное обеспечение следующие параметры событий:

- числовой идентификатор устройства, являющегося источником события;
- числовой идентификатор события;
- номер карты пользователя (только для событий, связанных с предъявлением карты);
- дата и время события.

Перечень событий, формируемых устройствами СКУД Elsys, приведён в приложении (п. 5.1). Текст событий может быть изменён и зависит от настроек системы и версии клиентского ПО.

1.4.3 Организация информационного обмена в СКУД Elsys

Контроллеры могут быть подключены в сеть СКУД Elsys одним из трёх способов:

- по двухпроводному интерфейсу RS-485 через преобразователь интерфейсов (Elsys-RC-232/485, Elsys-CU-USB/232-485), подключаемый к COM или USB порту ПК;
- 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 сервер интеграции может выполнять либо напрямую, либо через КСК).

Возможно использование всех перечисленных выше вариантов построения системы в любом сочетании.

Сетевой обмен информацией между контроллерами и сервером интеграции обеспечивает:

- поиск устройств (контроллеров, КСК, считывателей, подключаемых по интерфейсу ESDP к контроллерам, устройств двухпроводной линии связи, подключаемых к охранным контроллерам Elsys-AC2) и назначение сетевых адресов оборудованию;
- загрузку в контроллеры и КСК аппаратных настроек и конфигурации охранной подсистемы;
- начальную загрузку базы данных пользователей СКУД и охранной подсистемы и их полномочий (инициализация пропусков);
- загрузку в контроллеры и КСК конфигурации зон доступа для работы глобального контроля последовательности прохода;
- обновление данных в контроллерах при изменении базы данных пользователей СКУД и охранной подсистемы и их полномочий (выдача и возврат пропусков, редактирование временных расписаний и уровней доступа и т. п.);

- передачу зарегистрированных контроллерами и КСК событий в управляющее программное обеспечение;
- передачи управляющих команд с рабочего места дежурного оператора в контроллеры.

Контроллеры могут выполнять обмен информацией между собой для обеспечения аппаратных функций – глобального контроля последовательности прохода и межконтроллерных взаимодействий. При использовании в составе СКУД Elsys КСК возможно создание единого информационного пространства, в пределах которого возможен обмен данными между контроллерами, включёнными в разные линии связи и/или в разные сетевые группы. На рисунке (Рисунок 3) приведена схема, иллюстрирующая взаимодействие оборудования СКУД Elsys с сервером интеграции и между собой при организации единого информационного пространства.

Контроллеры Elsys-NG-1000 и КСК Elsys-NG-Net II могут быть подключены к серверу интеграции по защищённому каналу с использованием протокола mTLS.

На рисунке (Рисунок 4) приведена схема, иллюстрирующая информационный обмен между сервером интеграции и оборудованием СКУД Elsys при использовании защищённых mTLS-соединений.

В таблице (Таблица 5) описаны функциональные особенности обмена данными при разных способах подключения.

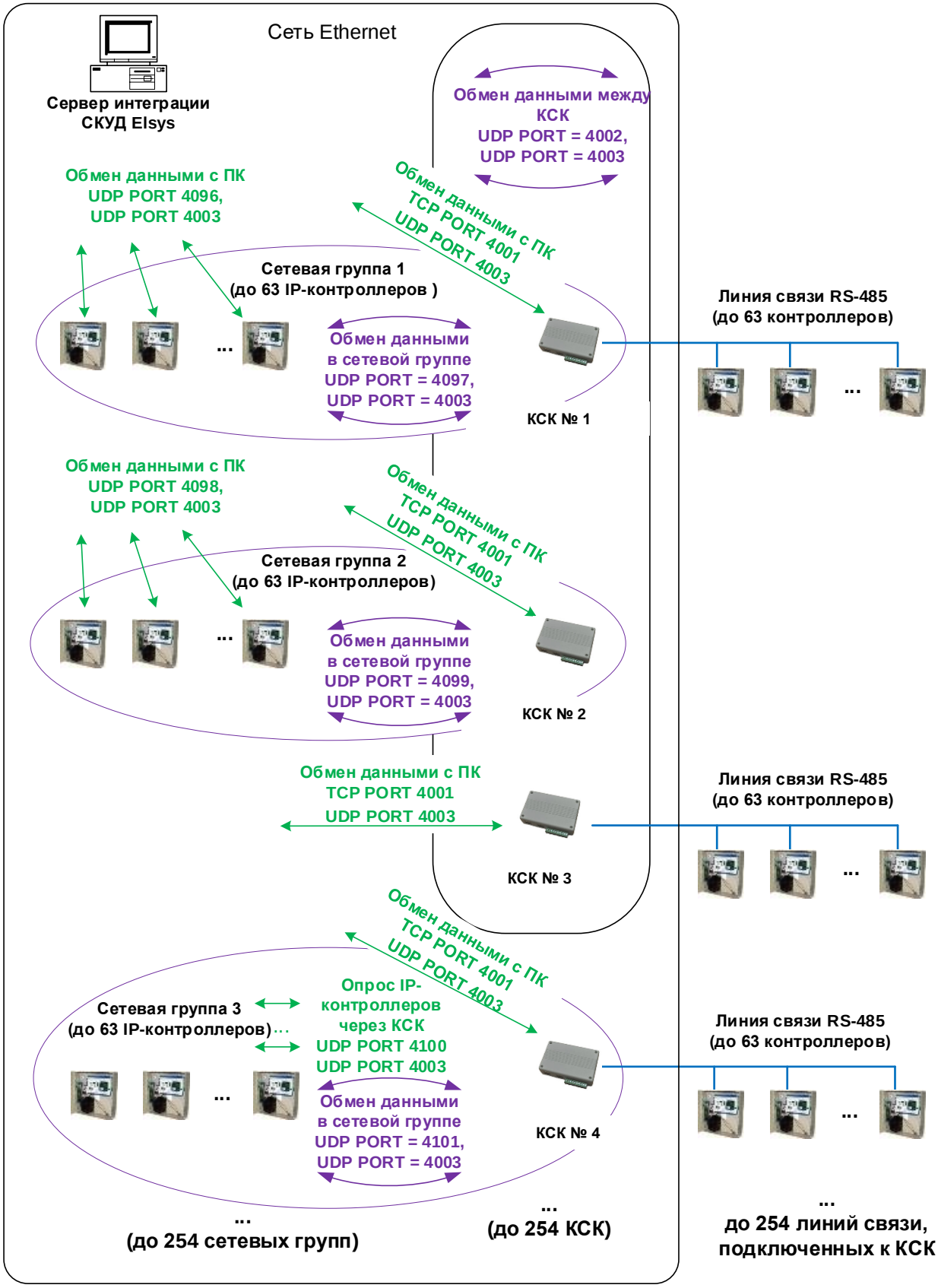

Рисунок 3. Обмен данными в СКУД Elsys при организации единого информационного пространства (mTLS-соединения не используются)

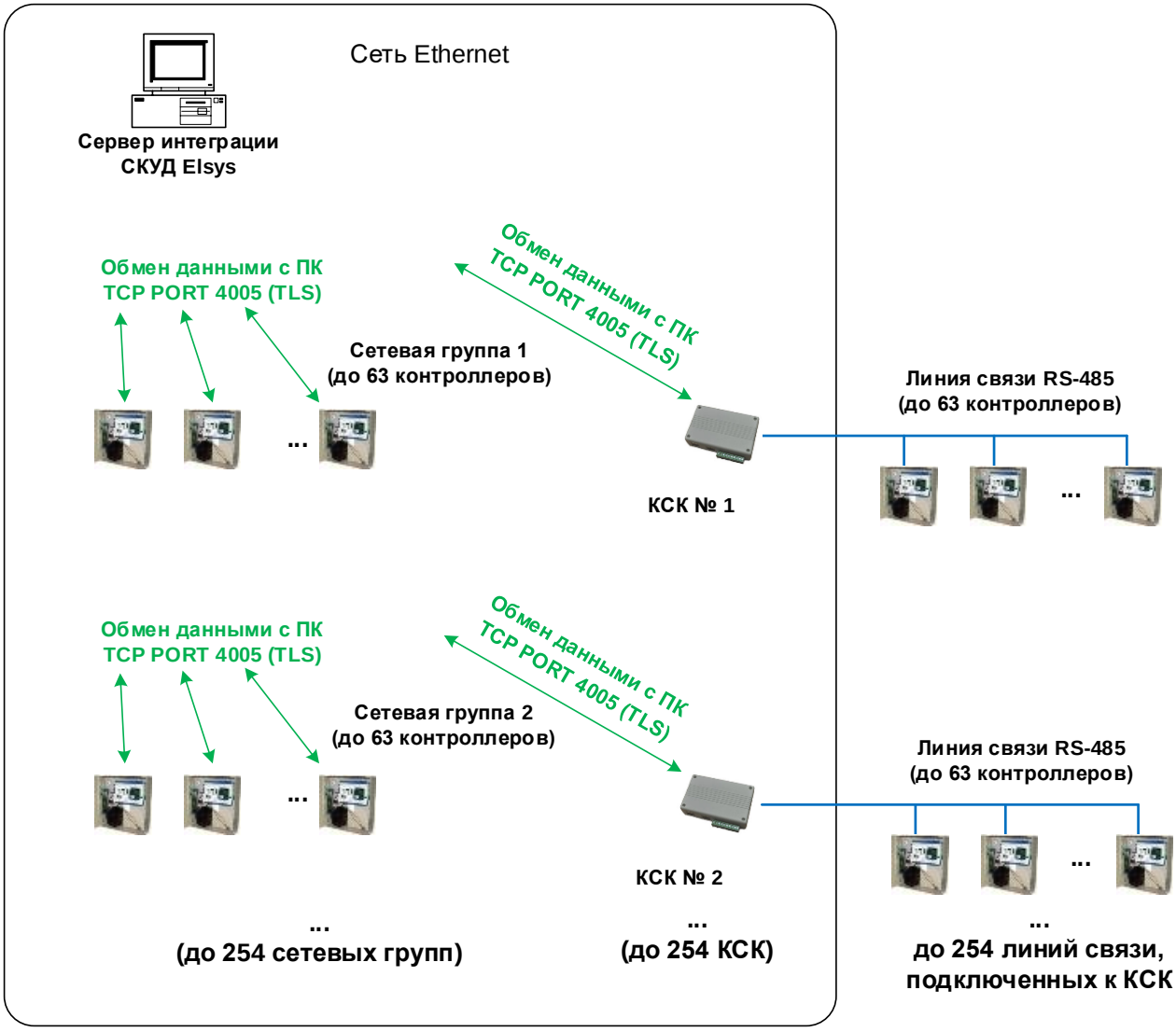

Рисунок 4. Обмен данными в СКУД Elsys
при использовании защищённых mTLS-соединений

Таблица 5.

Обмен данными при разных способах подключения оборудования СКУД Elsys

Способ подключения	**Обмен данными с сервером интеграции**	**Обмен данными с контроллерами, включёнными в общую линию связи или сетевую группу**	**Обмен данными с контроллерами, включёнными в другие линии связи или сетевые группы**
К последовательному или USB-порту ПК через преобразователи	Сервер интеграции выполняет опрос контроллеров в режиме MASTER/SLAVE или MULTIMASTER	Осуществляется при включенном в линии режиме MULTIMASTER	Обмен информацией невозможен

Способ подключения	**Обмен данными с сервером интеграции**	**Обмен данными с контроллерами, включёнными в общую линию связи или сетевую группу**	**Обмен данными с контроллерами, включёнными в другие линии связи или сетевые группы**
интерфейсов Elsys-RC-232/485, Elsys-CU-USB/232-485			
Через КСК, по RS-485. Режим mTLS в КСК выключен	Сервер интеграции выполняет опрос КСК по протоколу TCP, а КСК опрашивает контроллеры по RS-485 в режиме MASTER/SLAVE или MULTIMASTER	Осуществляется при включенном в линии RS-485 режиме MULTIMASTER	Обмен информацией осуществляется при включенном в линии RS-485 режиме MULTIMASTER через КСК, выполняющим обмен с другими КСК по протоколу UDP
Через КСК, по RS-485. Режим mTLS в КСК включен.	Сервер интеграции выполняет опрос КСК по протоколу TCP в режиме защищённого соединения mTLS, а КСК опрашивает контроллеры по RS-485 в режиме MASTER/SLAVE или MULTIMASTER.	Осуществляется при включенном в линии RS-485 режиме MULTIMASTER.	Обмен информацией невозможен
Ethernet. Режим mTLS в контроллерах и КСК выключен	Возможно два способа опроса контроллеров: 1. Сервер интеграции опрашивает контроллеры по протоколу UDP; 2. Сервер интеграции выполняет опрос КСК по протоколу TCP, а КСК опрашивает контроллеры по протоколу UDP.	До 63 контроллеров объединяются в сетевую группу, в пределах которой возможен обмен данными по протоколу UDP	Обмен информацией осуществляется по протоколу UDP через КСК, включенный в сетевую группу и выполняющий обмен информацией с другими КСК по протоколу UDP
Ethernet. Режим mTLS в контроллерах и КСК включен	Сервер интеграции опрашивает контроллеры по протоколу TCP в режиме защищённого соединения mTLS	Обмен информацией невозможен	Обмен информацией невозможен

1.4.4 Точки доступа

В СКУД Elsys поддерживаются точки доступа следующих типов:

- дверь;
- турникет;
- ворота (шлагбаум).

В состав оборудования точек доступа входят считыватели, датчики прохода и исполнительные устройства (замки, турникеты, приводы управления шлагбаумами и воротами).

Каждый контроллер, в зависимости от типа и варианта исполнения, может обслуживать до четырёх дверей, ворот или шлагбаумов, либо до двух турникетов.

При использовании иных управляемых преграждающих устройств (электромеханические калитки, шлюзовые кабины и т. п.) следует выбирать наиболее близкий по алгоритму работы тип точки доступа, либо использовать несколько точек доступа, настраивая требуемым образом алгоритм их взаимодействия.

Режимы работы точек доступа описаны в таблице (Таблица 6). Управляющие команды для точек доступа приведены в приложении (п. 5.2, Таблица 21, Таблица 22, Таблица 23).

Таблица 6.

Режимы работы точек доступа

Тип точки доступа	**Режим работы**	**Описание**
Дверь	Нормальный режим	Доступ осуществляется в обычном режиме. Несанкционированное открывание вызывает событие «Взлом».
	Разблокировка	УПУ обеспечивают свободный проход. Если замок электромеханический, то после каждого закрывания (защёлкивания) двери выполняется автоматическое её отпирание путём подачи импульса с длительностью, заданной в настройках этой двери. Если замок электромагнитный, то напряжение с него снимается на длительное время (управляющий выход постоянно включен). Штатный проход регистрируется в момент предъявления карты.

Тип точки доступа	Режим работы	Описание
	Блокировка	Управляющие реле выключены, считыватели заблокированы, доступ запрещён всем без исключения
Турникет	Нормальный режим	Аналогично соответствующим режимам для двери
	Разблокировка	
	Блокировка	
	Нормальный режим на вход, заблокировано на выход	Для каждого из направлений прохода – аналогично соответствующим режимам для двери
	Заблокировано на вход, нормальный режим на выход	
	Нормальный режим на вход, разблокировано на выход	
	Разблокировано на вход, нормальный режим на выход	
	Заблокировано на вход, разблокировано на вход	
	Разблокировано на вход, Заблокировано на вход	
Ворота (шлагбаум)	Нормальный режим	Аналогично соответствующим режимам для двери
	Блокировка	

1.4.5 Полномочия и настройки пользователей СКУД

Описание полномочий и настроек пользователей СКУД приведено в таблице (Таблица 7).

Таблица 7.

Идентификационные признаки и полномочия пользователей системы

Наименование настройки	Описание
Номер карты	Основной уникальный идентификационный признак, однозначно определяющий пользователя системы. Длина значащей части номера карты может составлять, в зависимости от типа контроллера и настроек системы, 3, 6 или 8 байт.
PIN-код	Дополнительный идентификационный признак, вводимый с клавиатуры. Хранится в памяти контроллера в виде числового значения. Диапазон значений 1 – 65534. Для совместимости с другим оборудованием, использующим PIN-коды, рекомендуется использовать диапазон значений 1 – 9999.
Номер уровня	Диапазон значений 1 – 16382.

Наименование настройки	Описание
доступа	Уровень доступа для системы в целом характеризует набор разрешённых считывателей точек доступа с назначенными для них временными блоками. В каждый контроллер загружается подмножество уровня доступа, в которое входят считыватели, обслуживаемые этим контроллером.
Временная карта	Признак карты с ограниченным сроком действия
Дата начала действия	Если опция «Временная карта» включена, то срок действия карты определяется параметрами «Дата начала действия» и «Дата окончания действия» (срок действия включает обе даты). Временные карты вступают в силу в момент даты начала действия. По окончании срока действия временная карта автоматически удаляется из памяти контроллера.
Дата окончания действия	
Не отслеживать последовательность прохода	Для пропусков, у которых включена эта опция, не отслеживается последовательность прохода

Помимо описанных выше, для пользователей СКУД могут быть заданы дополнительные опции, описание которых дано в таблице (Таблица 8). Эти опции могут быть заданы отдельно для разных контроллеров и сгруппированы в предварительно настроенные наборы данных – профили настроек персонала.

Таблица 8.

Дополнительные настройки пользователей системы

Наименование настройки	Описание
Доступ только по PIN-коду	Эти настройки определяют способ идентификации пользователя на считывателях, оборудованных встроенной клавиатурой. Если обе опции выключены, необходимо вводить оба идентификационных признака. Если включена опция «Доступ только по PIN-коду», то для получения доступа достаточно набрать PIN-код, а если включена опция «Доступ только по карте», для получения доступа достаточно предъявить карту.
Доступ только по карте	
Проход в режиме ограничения доступа	Если настройка включена, пользователю разрешён доступ, если считыватель находится в режиме ограничения доступа.
Право ставить на охрану	Эти опции позволяют выполнять пользователю действия по управлению охраной с помощью кнопки управления охраной либо путём удержания карты. Опция «Право ставить на охрану», кроме того, разрешает сотруднику использование служебных PIN-кодов.
Право снимать с охраны	
При предоставлении доступа	Одновременно с предоставлением доступа будет сформировано одно из заданных событий - «Действие 1», «Действие 2»,

Наименование настройки	Описание
формировать событие	«Действие 3», которое может быть использовано как источник события при программировании логики работы контроллера или в иных целях.
Не предоставлять доступ	Если эта опция включена, то карта может использоваться только для управления охраной и выполнения других действий. Доступ не предоставляется.
Полномочия	Варианты настройки – «Обычные» (по умолчанию), «Доступ с подтверждением», «Право подтверждать доступ» или «Право сопровождать». Если установлены полномочия «Доступ с подтверждением», то для предоставления доступа необходимо вслед за предъявлением данной карты предъявить карту с полномочиями «Право сопровождать» или «Право подтверждать доступ». Для сотрудников с полномочиями «Право сопровождать» при подтверждении доступа картой также будет предоставлен доступ (система зафиксирует проход двух сотрудников), а картам с полномочиями «Право подтверждать доступ» – нет (будет зафиксирован проход только первого сотрудника). Во всём остальном права этих двух групп полномочий соответствуют полномочиям «Обычные». Если для считывателя включена опция «Подтверждать доступ для карт, требующих подтверждения», то для карт с полномочиями «Доступ с подтверждением» подтверждение осуществляется только кнопкой дежурного оператора «Подтверждение доступа».

1.4.6 Временные расписания

Временные расписания (далее – временные блоки) используются для разграничения полномочий пользователей СКУД по времени. В составе уровня доступа различные временные блоки могут быть назначены для разных считывателей. Временные блоки могут состоять из произвольного количества временных интервалов. Максимальное количество интервалов во временном блоке ограничено только числовыми характеристиками контроллера (см. таблицу (Таблица 2), параметр «Количество временных интервалов»).

Каждый временной интервал, входящий во временной блок, описывается следующими параметрами:

- номер временного блока, к которому относится описываемый временной интервал (диапазон значений от 1 до 16382);
- начало временного интервала (часы, минуты);

- окончание временного интервала (часы, минуты);
- периодичность графика (от 2 до 31, значение 7 соответствует недельному графику);
- дата начала работы временного интервала (для скользящих графиков одновременно является опорной датой, относительно которой отсчитываются дни графика; для недельного графика анализируется при условии, что задана дата окончания работы временного интервала);
- дата окончания работы временного интервала (не анализируется, если не задана или равна дате начала работы временного интервала);
- активные дни графика (дни недели – для недельных графиков, дни с номерами от 1 до 31 – для скользящих графиков; праздничные дни двух типов).

Время окончания интервала должно быть больше времени его начала. Если интервал переходит суточную границу (например, «21.00 – 05.29»), его следует разбивать на два интервала («21.00 – 23.59» и «0.00 – 5.29»). Временной интервал считается активным, если текущее время находится внутри границ временного интервала, и если текущий день относится к списку разрешённых дней графика для этого временного интервала. Временной блок считается активным, если хотя бы один временной интервал, входящий в его состав, активен.

Номером текущего дня является:

- номер дня недели, если график недельный;
- номер дня относительно опорной даты, если график скользящий.

Если текущая дата содержится в списке праздничных дней, номер дня определяется в соответствии с типом праздничного дня.

В списке праздничных дней задаются все исключения из графиков (до 32). Любой календарный день года может быть задан как праздник первого или второго типа, а также назначен как любой из дней недели. Так, если необходимо перенести выходной (воскресенье) с 4 на 2 мая (1 мая – праздничный день), достаточно назначить в таблице праздничных дней для 1 и 2 мая режим воскресенья, а для 4 мая – режим понедельника.

1.4.7 Контроль последовательности прохода

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

В режиме локального контроля последовательности прохода контроллер отслеживает местоположение пользователя в пределах двух зон, разделённых одной или двумя точками доступа, обслуживаемыми контроллером.

Глобальный аппаратный контроль последовательности прохода функционирует в пределах единого информационного пространства, в котором возможен обмен информацией между контроллерами. Единое информационное пространство может быть организовано в пределах одной линии связи RS-485 или сетевой группы (до 63 контроллеров), а при использовании КСК – в совокупности всех контроллеров, обслуживаемых ими. В едином информационном пространстве глобальный контроль последовательности прохода работает децентрализовано, без участия компьютера.

Внимание! Аппаратная реализация глобального контроля последовательности прохода недоступна при использовании защищённых сетевых протоколов mTLS, TLS.

Глобальный программный контроль последовательности прохода функционирует при условии непрерывной работы сервиса интеграции – программного обеспечения, выполняющего обмен информацией с оборудованием и взаимодействующего с клиентским программным обеспечением. Глобальный программный контроль последовательности прохода следует использовать в случае невозможности организовать обмен информацией между контроллерами системы (при использовании защищённых сетевых протоколов mTLS, TLS; при невозможности использовать UDP-обмен в сети Ethernet или режим Multimaster в линии RS-485).

Функциональные возможности глобального контроля последовательности прохода, описанные ниже, актуальны как для аппаратной, так и для программной реализации этой функции.

В режиме глобального контроля последовательности прохода контроллеры Elsys-MB-Pro4, Elsys-NG-800 и Elsys-NG-1000 могут обслуживать

до четырёх зон доступа, остальные контроллеры доступа до двух зон (для обозначения зон доступа также используются термины «область контроля», «территория»). Структура зон доступа (вложенность и т. п.) ничем не ограничена.

Если контроль последовательности прохода включен, то контроллер, анализируя сообщения от других контроллеров и КСК, непрерывно обновляет в своей памяти информацию о местоположении пользователей системы, а также отправляет для обработки другим контроллерам информацию о регистрируемых событиях. Информация о текущем местоположении пользователей используется контроллерами при принятии решения о предоставлении доступа.

Пользователь, находящийся в одной из зон доступа, имеет право на выход из этой зоны во всех точках доступа, ограничивающих эту зону. Если этот пользователь предъявит карту в любой другой зоне доступа, в доступе ему будет отказано с регистрацией сообщения «Нарушение зоны доступа».

Если местоположение пользователя неизвестно (после начальной загрузки данных, после длительного отсутствия связи с другими контроллерами, после сброса или включения питания и др.), доступ разрешается в любых направлениях.

Опция контроллера *«Сброс в полночь»*, если она включена, обеспечивает ежесуточный сброс в 0 ч 0 мин зон доступа всех пользователей.

В зависимости от настроек контроллера, возможно использование дополнительных опций при работе контроля последовательности прохода:

- «Временной antipassback»;
- «Усиленный antipassback».

Опция «Временной antipassback» обеспечивает автоматический сброс текущего местоположения пользователя через заданное время (устанавливается в настройках контроллера) после совершения последнего прохода.

Опция «Усиленный antipassback» обеспечивает защиту от действий злоумышленников, пытающихся совершить проход нескольких лиц путём предъявления одной карты считывателям нескольких точек доступа (например, на турникетах проходной предприятия). Если включена опция «Усиленный antipassback», контроллеры системы в момент предъявления карты

регистрируют изменение местоположение пользователя, а в случае, если проход не состоялся, восстанавливают реальное местоположение пользователя.

1.4.8 Встроенные алгоритмы прохода

1.4.8.1 Проход по карте доступа

После предъявления карты считывателю контроллер анализирует полномочия пользователя и принимает решение о предоставлении доступа или отказе в доступе. Если доступ предоставлен, в точке прохода регистрируется событие «Предоставление доступа на вход» либо «Предоставление доступа на выход», в зависимости от направления прохода.

После предоставления доступа выполняется шунтирование датчика прохода и включение управляющего реле на заданное время. Затем, по срабатыванию датчика прохода, регистрируется событие «Штатный вход» или «Штатный выход» соответственно. Эти события могут быть зарегистрированы немедленно в следующих случаях:

- выключена опция точки доступа «Отслеживать фактический проход»;
- точка доступа находится в режиме разблокировки;
- точка доступа находится в состоянии «Открыто», «Удержание», «Взлом».

В случае отказа в доступе будет сформировано событие, соответствующее причине отказа.

Если считыватель оборудован также клавиатурой, проход по карте возможен лишь в том случае, если у пользователя активна опция «Доступ только по карте».

1.4.8.2 Проход по карте доступа и PIN-коду

В этом режиме необходимо предварительно набрать на клавиатуре считывателя PIN-код (ввод числового значения должен завершаться нажатием кнопки «*»), а затем, через время, не превышающее «Интервал между набором кода и предъявлением карты» (настройка считывателя), предъявить карту доступа. В остальном алгоритм идентичен алгоритму прохода по карте доступа.

Для реализации данного алгоритма необходимо, чтобы в настройках контроллера была включена опция «Использовать PIN-коды», а используемый считыватель был оборудован клавиатурой.

1.4.8.3 *Проход по PIN-коду*

В этом режиме необходимо предварительно набрать на клавиатуре считывателя PIN-код, и затем, после выполнения анализа полномочий пользователя будет выполнено предоставление доступа либо отказ в доступе. В остальном алгоритм идентичен алгоритму прохода по карте доступа.

Для реализации данного алгоритма необходимо, чтобы в настройках контроллера была включена опция «Использовать PIN-коды», а используемый считыватель был оборудован клавиатурой. Кроме того, в дополнительных настройках пользователя должна быть включена опция «Только PIN», а для контроллеров линейки Elsys-NG-xx должна быть выключена опция «Не использовать PIN-код в качестве единственного идентификатора».

1.4.8.4 *Проход под принуждением*

Проход под принуждением – особый режим, смысл которого в том, что пользователь, открывающий под угрозой насилия дверь, может ввести модифицированный PIN-код. Внешне процедура прохода ничем не будет отличаться от обычной, однако вместо события «Штатный вход/выход» будет сформировано и передано на пост охраны тревожное событие «Вход/Выход под принуждением». Использование этого режима возможно при тех же условиях, что и использование режима «Проход по карте доступа и PIN-коду». На считывателях, где предполагается использовать проход под принуждением, необходимо включить опцию «Используется вход под принуждением».

«Принудительный» PIN-код отличается от штатного младшей цифрой, которая вычисляется следующим образом: если младшая цифра PIN-кода в диапазоне 0 – 4, необходимо прибавить число 5, если младшая цифра в диапазоне 5 – 9, необходимо отнять число 5. При использовании доступа под принуждением необходимо проследить, чтобы ни один «принудительный» код не совпадал со штатным PIN-кодом. Например, диапазонам штатных PIN-кодов: 1 – 4, 15 – 24 и 35 – 44 соответствуют диапазоны «принудительных» PIN-кодов: 6 – 14, 25 – 34 и 45 – 49.

1.4.8.5 *Проход с подтверждением и проход с сопровождением*

Для организации этого режима одной группе сотрудников следует задать полномочия «Доступ с подтверждением», а другой – «Право сопровождать»

или «Право подтверждать доступ». Алгоритм работы контроллера при этом будет следующий. Пользователь с полномочиями «Доступ с подтверждением» первым предъявляет карту доступа. Контроллер проверяет его полномочия, и, если нет оснований для отказа в доступе, формирует событие «Требуется подтверждение доступа при входе/выходе». Затем, в течение интервала времени, не превышающем «Интервал при предъявлении нескольких карт» (настройка считывателя), второй сотрудник должен предъявить свою карту. Если будет предъявлена неверная карта, будет сформировано событие «Отказ в доступе на вход/выход – нет полномочий».

Если второй будет предъявлена карта с полномочиями «Право сопровождать», будут сформированы два события «Предоставление доступа на вход/выход», с номерами первой и второй карты, а затем, после срабатывания датчика прохода, будут сформированы соответственно два события «Штатный вход/выход», и оба пользователя будут считаться прошедшими.

Если второй будет предъявлена карта с полномочиями «Право подтверждать доступ», то будут сформированы два события – «Подтверждение доступа картой при входе/выходе» и «Предоставление доступа на вход/выход» с номером первой карты. Затем, после срабатывания датчика прохода, будет сформировано событие «Штатный вход/выход» с номером первой карты, т. е. прошедшим будет считаться только первый сотрудник.

1.4.8.6 Проход с подтверждением кнопкой оператора

Для организации этого режима доступа необходимо в настройках считывателя назначить «Вход для подтверждения доступа» и «Вход для отказа в доступе» (второе – не обязательно), к которым соответственно будут подключаться кнопки подтверждения и отказа в доступе. Если точка доступа двусторонняя, каждая из кнопок может быть назначена для обоих считывателей.

Кроме того, следует задать набор полномочий дежурного оператора, в который могут входить права:

- «Подтверждать доступ для нарушивших временную зону»;
- «Подтверждать доступ при любых нарушениях режима доступа» (т. е. для нарушивших временные расписания либо для нарушивших последовательность прохода);

– «Подтверждать доступ для карт с полномочиями «Доступ с подтверждением».

При предъявлении карты будет сформировано событие «Требуется подтверждение доступа при входе/выходе». Если было нарушение режима доступа, будет также сформировано одно из событий «Нарушение временной зоны» или «Нарушение зоны доступа» (в этих случаях событие «Требуется подтверждение доступа при входе/выходе» в протоколе не регистрируется, но на него могут быть назначены аппаратные реакции).

В момент нажатия оператором кнопки подтверждения формируются события «Подтверждение доступа оператором» и «Предоставление доступа».

1.4.8.7 Доступ по правилу двух (трёх) лиц

В помещениях с повышенными требованиями к пропускному режиму может быть использован алгоритм доступа по правилу двух (трёх) лиц. Этот алгоритм доступа может быть включен и настроен отдельно на каждом считывателе.

Для использования алгоритма доступа по правилу двух (трёх) лиц необходимо установить опцию считывателя «Необходимое количество карт для получения доступа» в одно из двух значений: «Две карты» или «Три карты». Для каждой из последовательно предъявляемых карт могут быть заданы необходимые для получения доступа опции, из набора значений:

– «Любая карта»;
– «Карта с опцией «Действие 1»;
– «Карта с опцией «Действие 2»;
– «Карта с опцией «Действие 3».

Если включена настройка считывателя «Учитывать последовательность предъявления карт», карты следует предъявлять в строго определённом порядке, в зависимости от необходимых опций. Если же эта настройка выключена, карты можно предъявлять в произвольном порядке. Максимальный интервал между предъявлениями карт задаётся настройкой считывателя «Интервал при предъявлении нескольких карт».

В момент успешного предъявления каждой карты формируются вспомогательные события «Предъявлена первая карта», «Предъявлена вторая карта», «Предъявлена третья карта». Эти события не регистрируются в

протоколе, но могут быть использованы для назначения аппаратных реакций, что обеспечивает организацию различных режимов индикации.

Если необходимое количество карт успешно предъявлено, контроллер предоставляет доступ, при этом в протоколе регистрируются события «Предоставление доступа» с кодами каждой из предъявленных карт. Затем, в момент фактического прохода, регистрируются события «Штатный вход/выход», с кодами каждой из предъявленных карт.

Если был нарушен порядок предъявления карт, либо полномочия карт не соответствовали требуемым, будут сформированы события «Отказ в доступе на вход/выход – нет полномочий» с кодами всех предъявленных карт. В случае, если своевременно не была предъявлена очередная карта доступа, будут сформированы события «Ошибка ввода очередной карты при входе/выходе» с кодами уже предъявленных карт.

1.4.8.8 «Мягкие» режимы контроля доступа

Нередко возникает необходимость не отказывать в доступе нарушителям пропускного режима, а разрешать доступ, одновременно регистрируя нарушение.

При включении опции считывателя «Предоставлять доступ при нарушении зоны доступа» нарушители последовательности прохода получают право доступа, при этом одновременно регистрируются два события – «Нарушение зоны доступа» и «Предоставление доступа».

Опция «Предоставлять доступ при нарушении временной зоны» в сочетании с настройкой «Допустимое опоздание» (возможные значения 5, 10, 15, 20, 30, 45, 60, 90, 120, 180 мин, «любое») позволяет задать допустимое отклонение от заданного временного расписания, при котором предоставляется доступ с одновременной регистрацией нарушения.

1.4.9 Охранные функции СКУД Elsys

В составе СКУД Elsys охранные функции могут выполнять как специализированные охранные приборы (охранные контроллеры Elsys-AC2, Elsys-MB-AC, клавиатуры Elsys-CP2), так и контроллеры доступа и КСК.

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.

При использовании централизованного управления охранной сигнализацией КСК Elsys-MB-Net II (или Elsys-NG-Net II), выполняющий функции центрального контроллера охранной сигнализации, 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).

Описание работы и порядок настройки технических средств охранной сигнализации, входящих в состав СКУД Elsys, приведено в документе «ТСОС Elsys. Руководство по эксплуатации».

1.4.10 Алгоритмы индикации считывателей

Настоящий раздел распространяется на контроллеры доступа Elsys-MB (кроме Elsys-MB-SM), Elsys-NG-200, Elsys-NG-800, Elsys-NG-1000. Описание алгоритмов индикации считывателей охранных контроллеров Elsys-MB-AC и Elsys-AC2 дано в соответствующих руководствах по эксплуатации.

Контроллер обеспечивает управление световой и звуковой индикацией считывателя (зелёный и красный светодиоды и звуковой излучатель) и отображение на этих индикаторах:

– состояния точки доступа и/или состояния назначенного для индикации охранного раздела (в зависимости от настроек);
– событий, связанных с действиями пользователя СКУД (предоставление доступа, отказ в доступе, управление режимами охраны и др.; для событий предусмотрена индикация в течение 0,5 – 2 с).

Алгоритмы индикации считывателей описаны в таблицах (Таблица 9, Таблица 10, Таблица 11).

Таблица 9.

Индикация состояний точки доступа

Состояние точки доступа	**Алгоритм индикации**
Нормальный режим	Включен красный
Дверь открыта или разблокирована	Включен зелёный

Состояние точки доступа	Алгоритм индикации
Взлом	Мигает красный по алгоритму «0,2 с включено/0,2 с выключено». Если включена опция считывателя *«Звук при взломе или удержании»*, звуковой сигнализатор работает по алгоритму «0,2 с включено/0,2 с выключено».
Удержание	Мигает жёлтый по алгоритму «два импульса по 0,1 с, с паузами по 0,1 с, с периодом 1 с». Если включена опция считывателя *«Звук при взломе или удержании»*, звуковой сигнализатор работает по алгоритму «два импульса по 0,1 с, с паузами по 0,1 с, с периодом 1 с».
Заблокировано	Мигает красный по алгоритму «0,9 с включено/0,1 с выключено»
Ожидание подтверждения доступа или предъявления следующей карты	Мигает зелёный по алгоритму «0,1 с включено/0,4 с выключено»

Таблица 10.

Индикация состояний охранного раздела

Приоритет состояния	Состояние	Алгоритм индикации
1	Тревога	Мигает красный и работает звуковой сигнализатор считывателя с частотой 2,5 Гц (по алгоритму «0,2 с включено/0,2 с выключено»)
2	Задержка тревоги	Мигает красный и работает звуковой сигнализатор считывателя по алгоритму «три импульса по 0,1 с, с паузами по 0,1 с, с периодом 1 с»
3	Невзятие	Мигает красный и работает звуковой сигнализатор считывателя по алгоритму «два импульса по 0,1 с, с паузами по 0,1 с, с периодом 1 с»
4	Задержка постановки на охрану – неготовность	Мигает красный и работает звуковой сигнализатор считывателя по алгоритму «два импульса по 0,1 с, с паузами по 0,1 с, с периодом 1 с»
5	Задержка постановки на охрану – норма	Мигает красный и работает звуковой сигнализатор считывателя по алгоритму «0,1 с включено/0,9 с выключено»
6	На охране	Включен красный
7	Дверь в составе раздела открыта или разблокирована	Включен зелёный

Приоритет состояния	Состояние	Алгоритм индикации
8	Неготовность охранного ШС	Включен жёлтый
9	Неготовность ШС типа «Объём»	Мигает жёлтый по алгоритму «два импульса по 0,1 с с паузами по 0,1 с периодом 1 с»
10	Неготовность входного ШС	Мигает жёлтый по алгоритму «0,1 с включено/0,9 с выключено»
11	Готовность	Для контроллеров доступа Elsys-MB, Elsys-NG-xx – все индикаторы выключены. Для охранных контроллеров – включен зелёный.
Примечание – В режиме индикации состояния охранного раздела состояние раздела определяется наиболее высокоприоритетным состоянием среди ШС, входящих в состав раздела (наиболее высокому приоритету соответствует самое низкое числовое значение приоритета). Кроме того, если раздел вне охраны, обеспечивается индикация открытого состояния входящей в состав раздела двери.		

Таблица 11.

Индикация событий

Событие	Алгоритм индикации
«Предоставление доступа», «Предоставление доступа под принуждением», «Предъявлена первая карта», «Предъявлена вторая карта», «Предъявлена третья карта»	С задержкой в 0,4 с формируется звуковой сигнал длительностью 0,3 с. Светодиод светится зелёным цветом в течение 1,5 с, либо, если осуществляется предоставление доступа, в течение времени, отводимого на проход.
«Нарушение временной зоны»	С задержкой в 0,4 с формируются два звуковых сигнала длительностью 0,1 с, с паузами по 0,1 с, сопровождаемых синхронным миганием светодиода жёлтым цветом.
«Нарушение зоны доступа»	С задержкой в 0,4 с формируются три звуковых сигнала длительностью 0,1 с, с паузами по 0,1 с, сопровождаемых синхронным миганием светодиода жёлтым цветом.
«Неизвестная карта», «Отказ в доступе – нет прав», «Отказ в доступе – блокировка», а также другие события, связанные с отказом в доступе по иным причинам	С задержкой в 0,4 с формируются четыре звуковых сигнала длительностью 0,1 с, с паузами по 0,1 с, сопровождаемых синхронным миганием светодиода жёлтым цветом.
«Взятие раздела на охрану»	С задержкой в 0,4 с формируется звуковой сигнал длительностью 0,3 с. Светодиод светится зелёным цветом в течение 1 с.

Событие	Алгоритм индикации
«Снятие раздела с охраны»	С задержкой в 0,4 с формируются два звуковых сигнала длительностью 0,1 с, с паузами по 0,1 с, сопровождаемых синхронным миганием светодиода зелёным цветом.
«Неудачное взятие раздела на охрану»	С задержкой в 0,4 с формируются пять звуковых сигналов длительностью 0,1 с, с паузами по 0,1 с, сопровождаемых синхронным миганием светодиода жёлтым цветом.
Окончание задержки взятия раздела на охрану	Звуковой сигнализатор включается на 1 с

1.4.11 Программирование логики работы контроллеров

Система программируемых аппаратных взаимодействий, имеющаяся в контроллерах, обеспечивает возможность программирования аппаратных реакций на регистрируемые события. Взаимодействия настраиваются в конфигураторе СКУД Elsys и при инициализации загружаются в энергонезависимую память контроллеров.

Всего в память контроллера может быть занесено до 250 взаимодействий.

Каждая запись о назначенном взаимодействии содержит:

- код устройства, являющегося источником события;
- код события;
- код устройства, выполняющего назначенное действие (команду);
- код назначенного действия;
- дополнительные параметры выполняемого действия (могут отсутствовать), например, задержка при постановке на охрану, формула управления выходом;
- условие выполнения реакции в виде логической формулы (см. ниже).

К устройствам, на события от которых можно назначать реакции, относятся:

- входы контроллера;
- выходы контроллера;
- считыватели;
- точки доступа (двери, турникеты, ворота);
- разделы охранной сигнализации;
- контроллер (событие «Сброс»).

Кроме того, реакции могут быть назначены на:

- активность/неактивность временного блока (диапазон номеров 1 – 125);
- активность/неактивность логической формулы;
- событие, сформированное другим контроллером, с учётом его адреса и номера события (диапазон номеров 1 – 64). Анализ событий от других контроллеров возможен, если настроен обмен данными между контроллерами;
- изменение значения счётчика событий (равенство значению, равенство значению после увеличения, равенство значению после уменьшения);
- потерю или восстановление связи с другим контроллером и/или компьютером (при условии, что настроен обмен данными между контроллерами);
- предъявление одной из служебных карт (возможно задание до 48 таких карт) на заданном считывателе;
- предъявление карты с заданным уровнем доступа;
- ввод одного из служебных PIN-кодов (возможно задание до 16 таких PIN-кодов) на заданном считывателе;
- ввод одного из служебных PIN-кодов на заданном считывателе, сопровождающийся предъявлением карты.

В качестве реакций на события могут быть назначены команды по управлению следующими устройствами:

- входы контроллера;
- выходы контроллера;
- считыватели;
- двери, турникеты, ворота и шлагбаумы;
- разделы охранной сигнализации.

Кроме того, возможно назначение реакций:

- для передачи событий в сеть контроллеров (при условии, что настроен обмен данными между контроллерами);
- для изменения значения (увеличения, уменьшения, загрузки нового значения) счётчика событий.

При настройке взаимодействий могут использоваться логические формулы, формулы управления выходами и счётчики событий (до 8).

Логические формулы представляют собой набор двоичных состояний устройств, объединяемых логическими операциями «И», «ИЛИ», «Исключающее ИЛИ», «НЕ». В составе логических формул могут участвовать входы, выходы, считыватели, временные блоки, другие логические формулы. Логические формулы могут быть использованы как источники событий, так и в качестве условий для выполнения реакций.

Сравнительные характеристики возможностей программирования логики работы контроллеров приведены в таблице (Таблица 12).

Подробно программирование логики работы контроллеров описано ниже (см. п. 2.3).

Таблица 12.

Возможности программирования логики работы контроллеров

Наименование параметра	**Тип контроллера**				
	Elsys-MB с модулем расширения памяти, Elsys-NG-200, Elsys-NG-800, Elsys-NG-1000	**Elsys-MB без модуля расширения памяти**	**Elsys-AC2**	**Elsys-MB-AC**	**Elsys-RM-16C, Elsys-IO/MB**
Количество взаимодействий	250	100	250 (для версий ниже 1.05 – 50)	50	50
Количество формул управления выходами	32	16	16	16	16
Количество логических формул	48	20	–	–	–
Количество счётчиков событий	8	8	–	–	–
Количество служебных PIN-кодов	16	16	–	–	–

Наименование параметра	**Тип контроллера**				
	Elsys-MB с модулем расширения памяти, Elsys-NG-200, Elsys-NG-800, Elsys-NG-1000	**Elsys-MB без модуля расширения памяти**	**Elsys-AC2**	**Elsys-MB-AC**	**Elsys-RM-16C, Elsys-IO/MB**
Возможность использования временных расписаний во взаимодействиях	+	+	–	–	–
Возможность назначения реакций на карты с конкретным номером	+	+	–	–	–
Возможность назначения реакций на карты с заданным номером уровня доступа	+	+	–	–	–

2 Настройка системы

2.1 Порядок настройки системы

Настройку системы следует выполнять в следующем порядке:

- выполнить установку сервиса интеграции и настройку его параметров;
- выполнить установку конфигуратора СКУД Elsys и подключиться к сервису интеграции;
- выполнить, если необходимо, настройку протокола DHCP и защищённых соединений в конфигураторе, сервисе интеграции и оборудовании;
- выполнить в конфигураторе первоначальную настройку системы, создав её конфигурацию с основными параметрами и добавив в неё КСК, линии связи, контроллеры и другие устройства;
- настроить в конфигураторе параметры оборудования;

- выполнить в конфигураторе загрузку настроек в сервис интеграции и в оборудование;
- подключить клиентское программное обеспечение к сервису интеграции;
- выполнить импорт конфигурации системы из сервиса интеграции в клиентское программное обеспечение;
- выполнить в клиентском программном обеспечении первоначальную настройку базы данных пользователей СКУД и охранной подсистемы,
- задать в клиентском программном обеспечении конфигурацию зон доступа (областей контроля, территорий), если будет использоваться глобальный контроль последовательности прохода;
- загрузить в оборудование настройки, выполненные в клиентском программном обеспечении (база данных пользователей СКУД и охранной подсистемы, конфигурация зон доступа).

При дальнейшей работе системы загрузка в оборудование СКУД Elsys изменений в базе данных пользователей СКУД и охранной подсистемы, конфигурации зон доступа будет выполняться автоматически, без участия пользователя. Необходимым условием для этого является работа в круглосуточном режиме клиентского программного обеспечения, сервиса интеграции, оборудования и каналов связи между ними.

В дальнейшем, после внесения изменений в настройки оборудования, необходимо повторно выполнять загрузку настроек в контроллеры, в конфигурацию которых были внесены изменения.

В некоторых случаях после изменения настроек оборудования может потребоваться выполнение инициализации базы данных персонала в клиентском программном обеспечении или инициализация настроек оборудования в других контроллерах.

Описание пользовательского интерфейса конфигуратора дано в документе «Конфигуратор СКУД Elsys. Руководство пользователя».

2.2 Настройка оборудования

2.2.1 Первоначальная настройка системы

Сразу после создания новой конфигурации системы необходимо выполнить настройку общих параметров системы (см. Рисунок 5): указать пароль доступа СКУД Elsys и задать размер номеров карт доступа.

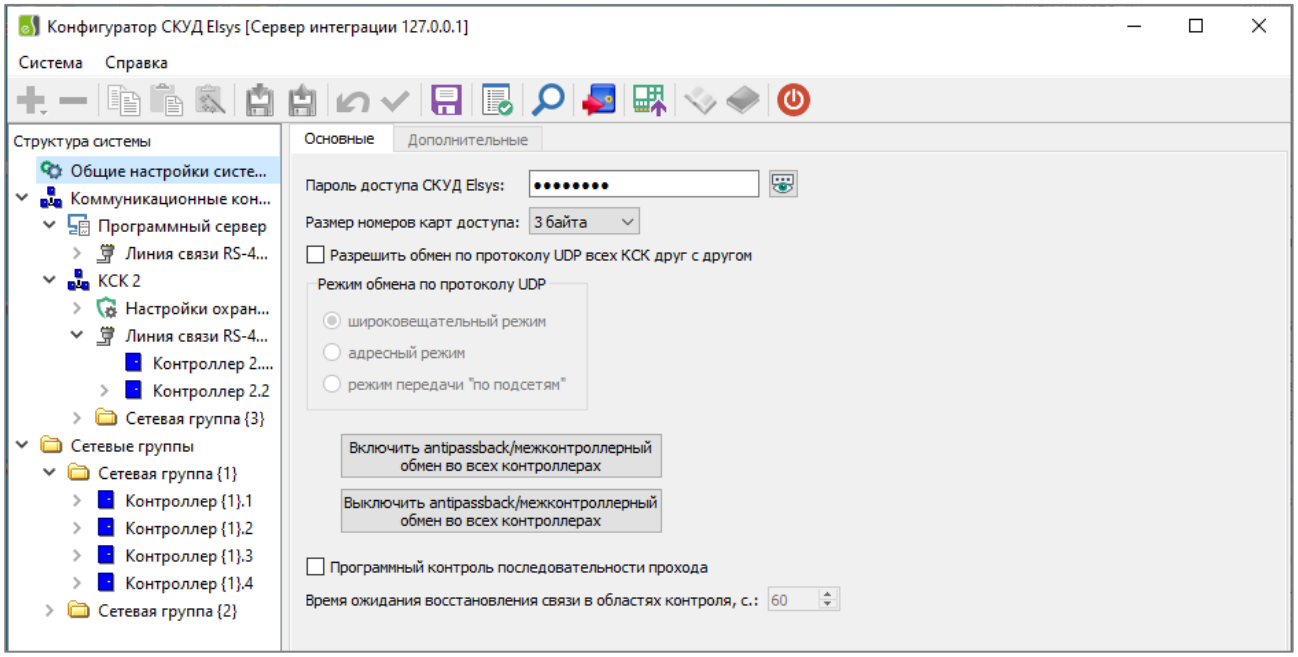

Рисунок 5. Окно общих настроек системы

Пароль доступа СКУД Elsys состоит из 8 символов. Допустимы любые печатаемые символы в кодировке ASCII (диапазон кодов символов 0x20…0x7F). Этот пароль используется сервисом интеграции и оборудованием СКУД Elsys при обмене информацией по сети Ethernet (кроме режима защищённого mTLS соединения), загружается в КСК и контроллеры при начальной настройке и хранится в их энергонезависимой памяти.

В дальнейшем пароль доступа СКУД Elsys может быть изменён. Процедура смены пароля описана в документе *«Конфигуратор СКУД Elsys. Руководство пользователя»*.

Внимание! Связь между сервисом интеграции, КСК и контроллерами в сети Ethernet (кроме режима защищённого mTLS соединения) возможна только при совпадении паролей в сервисе интеграции и устройствах, участвующих в обмене.

Возможные значения размера номера карт: 3, 6 или 8 байт. Необходимое значение рекомендуется установить до момента добавления контроллеров в систему. Иначе, после изменения настройки размера номеров карт потребуется:

- для добавленных ранее контроллеров Elsys-MB любых вариантов исполнения проверить и, при необходимости, скорректировать параметры формата базы данных (вкладка «Основные» в панели настройки параметров контроллера);
- для всех контроллеров (включая КСК и охранные контроллеры) выполнить в конфигураторе инициализацию настроек оборудования, а в клиентском ПО – инициализацию базы данных персонала и областей контроля.

Настройки «Разрешить обмен по протоколу UDP всех КСК друг с другом», «Режим обмена по протоколу UDP», «Программный контроль последовательности прохода», «Время ожидания восстановления связи в областях контроля», а также дополнительные параметры обмена информацией КСК, размещённые на вкладке «Дополнительные», описаны ниже (п. 2.2.7).

КСК и контроллеры могут быть добавлены в конфигурацию системы либо при выполнении процедуры поиска (см п. 2.2.2), либо в главном окне конфигуратора. При добавлении контроллеров доступа рекомендуется использовать поставляемые в комплекте с конфигуратором готовые конфигурации (см. п. 2.2.8.2).

2.2.2 Поиск устройств

2.2.2.1 Общие сведения

Функция поиска предназначена для обнаружения следующих видов оборудования:

- КСК, подключенных в общую сеть Ethernet с сервером интеграции, широковещательными или адресными запросами;
- контроллеров, подключенных к линиям связи RS-485 КСК, находящихся в общей с сервером интеграции сети Ethernet, запросами по адресам или серийным номерам;
- контроллеров, подключенных в общую с сервером интеграции сеть Ethernet, широковещательными или адресными запросами (передаваемыми либо непосредственно, либо через КСК, опрашиваемые сервером интеграции);

– устройств адресной двухпроводной линии связи (АДЛС) охранного контроллера Elsys-AC2;
– устройств, подключенных к контроллерам по протоколу ESDP.

Функция изменения сетевых настроек позволяет изменить адрес устройства (КСК или контроллера), номер сетевой группы (только для контроллеров с интерфейсом Ethernet) и параметры подключения к сети Ethernet (КСК и контроллеры с интерфейсом Ethernet). Для устройств АДЛС и ESDP доступна функция смены адреса устройства.

Поиск и изменение настроек в сети Ethernet возможен только для КСК и контроллеров, пароль которых не установлен либо совпадает с паролем сети СКУД Elsys сервера интеграции.

Форма поиска и изменения сетевых настроек оборудования (далее – форма поиска) вызывается с помощью кнопки на панели быстрого доступа (см. Рисунок 6).

Рисунок 6. Панель с кнопками быстрого доступа

Окно формы поиска имеет пять вкладок (см. Рисунок 7) — «Поиск КСК» (см. Рисунок 8), «Поиск контроллеров в линиях RS-485» (см. Рисунок 9), «Поиск контроллеров в сетевых группах» (см. Рисунок 10), «Поиск устройств АДЛС» (см. Рисунок 11) и «Поиск устройств ESDP» (см. Рисунок 12), предназначенных для использования процедур поиска и изменения параметров соответствующих видов оборудования.

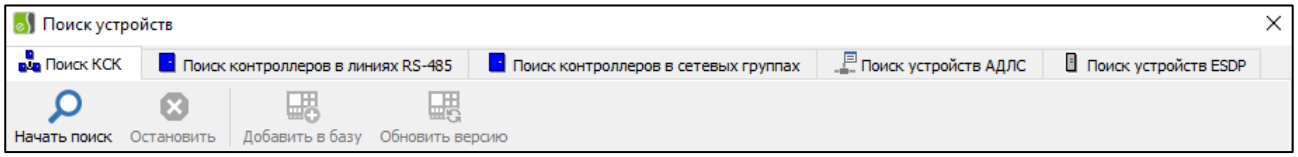

Рисунок 7. Вкладки окна формы поиска

Каждая вкладка имеет свою панель кнопок быстрого доступа, предназначенных для запуска процедуры поиска и прерывания запущенной процедуры поиска. Также на вкладках поиска КСК и контроллеров есть кнопки быстрого доступа для добавления обнаруженного оборудования в

конфигурацию системы (кнопка «Добавить в базу») и обновления ранее сохранённых параметров конфигурации устройства, таких как версия и тип устройства, тип модуля расширения контроллеров доступа. Обновление конфигурации системы для обнаруженных устройств АДЛС выполняется автоматически после завершения процесса поиска.

Несовпадение версий и типов модулей расширения отображается пиктограммой в одноимённом столбце таблицы (конфликт версий). Несовпадающие сетевые параметры (IP-адрес и/или маска подсети) отображаются пиктограммой в соответствующих столбцах таблицы (конфликт настроек).

2.2.2.2 *Поиск КСК*

Для поиска КСК в окне формы необходимо выбрать вкладку «Поиск КСК». При нажатии расположенной на панели быстрого доступа кнопки «Начать поиск» запускается процедура поиска широковещательными запросами. Для выполнения адресного поиска нужно указать искомый IP-адрес КСК в поле «Поиск по IP-адресу» и нажать расположенную рядом с ним кнопку.

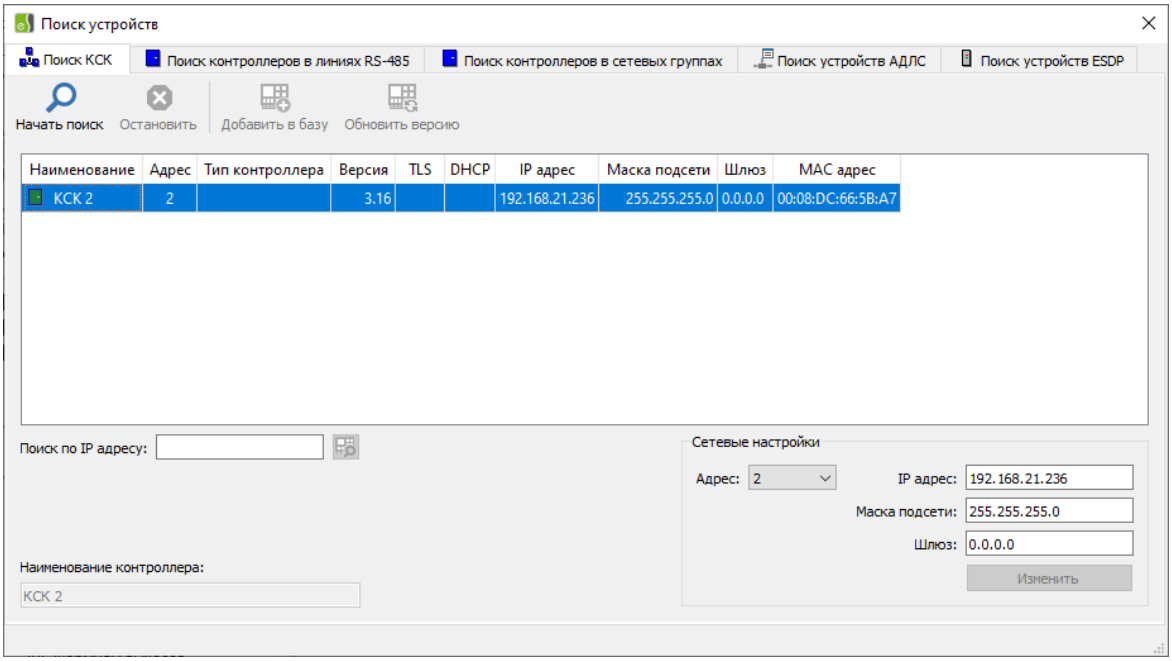

Рисунок 8. Окно формы поиска КСК

Процесс поиска может быть прерван по нажатию расположенной на панели быстрого доступа кнопки «Остановить».

Информация о найденных КСК отображается в табличном виде. Адреса найденных КСК проверяются на совпадение с адресами (номерами) КСК, уже существующими в конфигурации системы. При совпадении адресов перед условным наименованием КСК в таблице отображается пиктограмма  или  (существующий КСК), при несовпадении – пиктограмма  или  (новый КСК). Для существующих КСК также выполняется дополнительная сверка версии, IP-адреса и маски подсети.

КСК с настройками по умолчанию имеют IP-адрес 192.168.127.254. Такие КСК запрещено добавлять в конфигурацию системы, а их параметры должны быть настроены.

Настроить параметры как нового, так и существующего КСК, можно непосредственно из окна поиска. Для этого необходимо выделить в таблице строку с информацией об изменяемом КСК и указать нужные значения IP-адреса, маски подсети, адреса шлюза и адреса (номера) КСК в группе параметров «Сетевые настройки» внизу окна поиска и нажать кнопку «Изменить», после чего новые настройки будут записаны в КСК. Если выбранный пользователем номер КСК конфликтует с номером уже существующего КСК, то у пользователя будет запрошено подтверждение выполнения конфликтной операции. После смены настроек рекомендуется выполнить повторный поиск устройства для подтверждения изменений.

После изменения сетевых настроек выполняется повторная сверка информации о данном КСК с информацией, записанной в конфигурации системы.

Поле формы «Наименование контроллера» содержит условное наименование КСК. Для новых КСК наименование формируется автоматически на основе номера с возможностью ручного редактирования пользователем. Для существующих КСК условное наименование считывается из конфигурации системы и недоступно для редактирования пользователем.

После того как все настройки сделаны, новый КСК может быть добавлен в конфигурацию системы кнопкой «Добавить в базу».

Внимание! Если у КСК включен режим DHCP, то смена сетевых настроек, кроме номера КСК, невозможна. Если включена опция TLS, установить соединение возможно только в защищённом

режиме, при этом номер КСК роли не играет и может использоваться только для логического разделения устройств при поиске.

Для существующих КСК при конфликте версий можно выполнить процедуру обновления информации в конфигурации системы кнопкой «Обновить версию» после подтверждения запроса пользователем. При одновременном конфликте настроек и версий процедура обновления информации недоступна. В таком случае требуется либо изменение параметров КСК, либо исправление пользователем соответствующих параметров конфигурации системы.

2.2.2.3 Поиск в линии RS-485

Для поиска контроллеров, подключенных к линиям связи RS-485 КСК, находящихся в общей с сервером интеграции сети Ethernet, а также к линии связи RS-485, подключенной к серверу интеграции, необходимо выбрать вкладку «Поиск контроллеров в линиях RS-485». При нажатии расположенной на панели быстрого доступа формы кнопки «Начать поиск» запускается процедура поиска контроллеров по адресам, либо по серийным номерам. Текущий метод поиска определяется состоянием флага «Поиск по серийному номеру». Поиск контроллеров осуществляется отдельно для каждой линии связи RS-485. Выбор линии связи, в которой будет выполняться поиск, осуществляется в выпадающем списке «Искать подключенные к…» (см. Рисунок 9). Установка скорости обмена, на которой будет выполняться поиск, выполняется с помощью выпадающего списка «Скорость обмена». Если поиск выполняется на скорости, отличающейся от заданной в свойствах КСК, по окончании поиска для найденных устройств (при условии, если для них возможна программная смена скорости обмена) будет выполнено переключение скорости обмена на скорость, заданную в свойствах КСК. Программная смена скорости обмена возможна для контроллеров, не оснащённых DIP-переключателями (Elsys-AC2, Elsys-CP2), либо при условии, что все DIP-переключатели, устанавливающие скорость обмена, выключены.

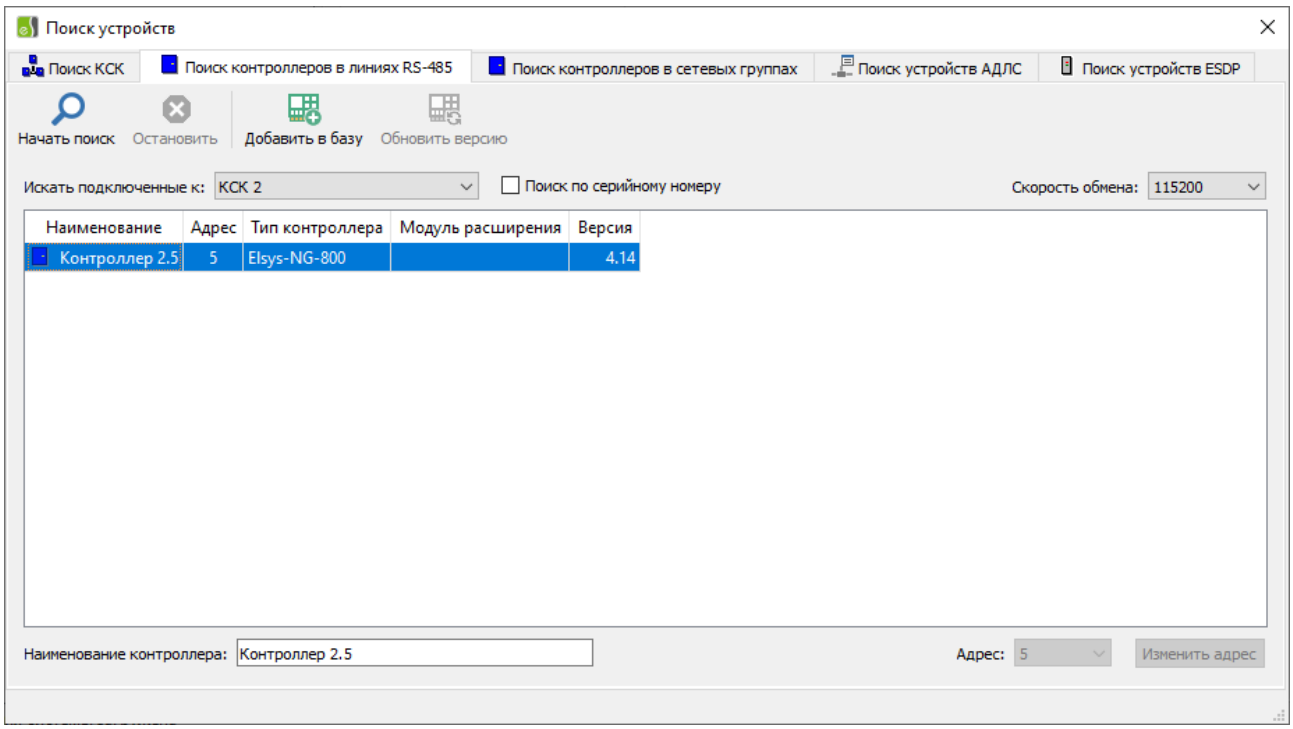

Рисунок 9. Окно формы поиска контроллеров с интерфейсом RS-485

Процесс поиска может быть прерван по нажатию расположенной на панели быстрого доступа формы кнопки «Остановить».

Информация о найденных контроллерах отображается в табличном виде. Адреса найденных контроллеров проверяются на совпадение с адресами контроллеров, уже существующих в конфигурации системы. При совпадении адресов перед условным наименованием контроллера в таблице отображается пиктограмма (существующий контроллер), при несовпадении – пиктограмма (новый контроллер). Для существующих контроллеров также выполняется дополнительная сверка версии, типа (варианта исполнения) и типа модуля расширения (для контроллеров доступа).

Настроить адрес как нового, так и существующего контроллера, можно непосредственно из окна поиска при условии, что для данного контроллера эта операция разрешена. Для этого нужно выделить в таблице строку контроллера, адрес которого необходимо изменить, указать новое значение адреса контроллера в выпадающем списке «Адрес» внизу окна поиска и нажать кнопку «Изменить адрес», после чего новые настройки будут записаны в контроллер. Присваиваемые контроллерам адреса в одной линии связи RS-485 должны идти по порядку без пропусков и принимать значение от 1 до 63 и не должны повторяться.

Поле формы «Наименование контроллера» для новых контроллеров заполняется автоматически генерируемым наименованием с возможностью ручного редактирования пользователем. Для существующих контроллеров условное наименование считывается из конфигурации системы и недоступно для редактирования пользователем.

После того как все настройки сделаны, новый контроллер может быть добавлен в конфигурацию системы кнопкой «Добавить в базу». Если для добавляемого контроллера существует хотя бы одна готовая конфигурация, то будет предложено выбрать готовую конфигурацию, совместимую с его типом или вариантом исполнения. При отказе от выбора, либо при отсутствии готовой конфигурации, контроллер будет добавлен с пустой конфигурацией.

Для существующих контроллеров при конфликте версий можно выполнить процедуру обновления информации в конфигурации системы кнопкой «Обновить версию» после подтверждения запроса пользователем. При одновременном конфликте версий и типов процедура обновления информации недоступна.

2.2.2.4 Поиск IP-контроллеров

Для поиска контроллеров, подключенных в общую с сервером интеграции сеть Ethernet, необходимо выбрать вкладку «Поиск контроллеров в сетевых группах» (см. Рисунок 10).

При нажатии расположенной на панели быстрого доступа формы кнопки «Начать поиск» запускается процедура поиска широковещательными запросами. Для выполнения адресного поиска нужно указать искомый IP-адрес контроллера в поле «Поиск по IP-адресу» и нажать расположенную рядом с ним кнопку  . Для ограничения диапазона поиска можно установить флаг «Искать в заданной сетевой группе» и выбрать нужный номер сетевой группы в расположенном ниже выпадающем списке. Для поиска через КСК, опрашиваемые сервером интеграции, необходимо установить флаг «Искать через управляющий КСК» и выбрать нужный КСК в расположенном ниже выпадающем списке. Процесс поиска может быть прерван по нажатию расположенной на панели быстрого доступа формы кнопки «Остановить».

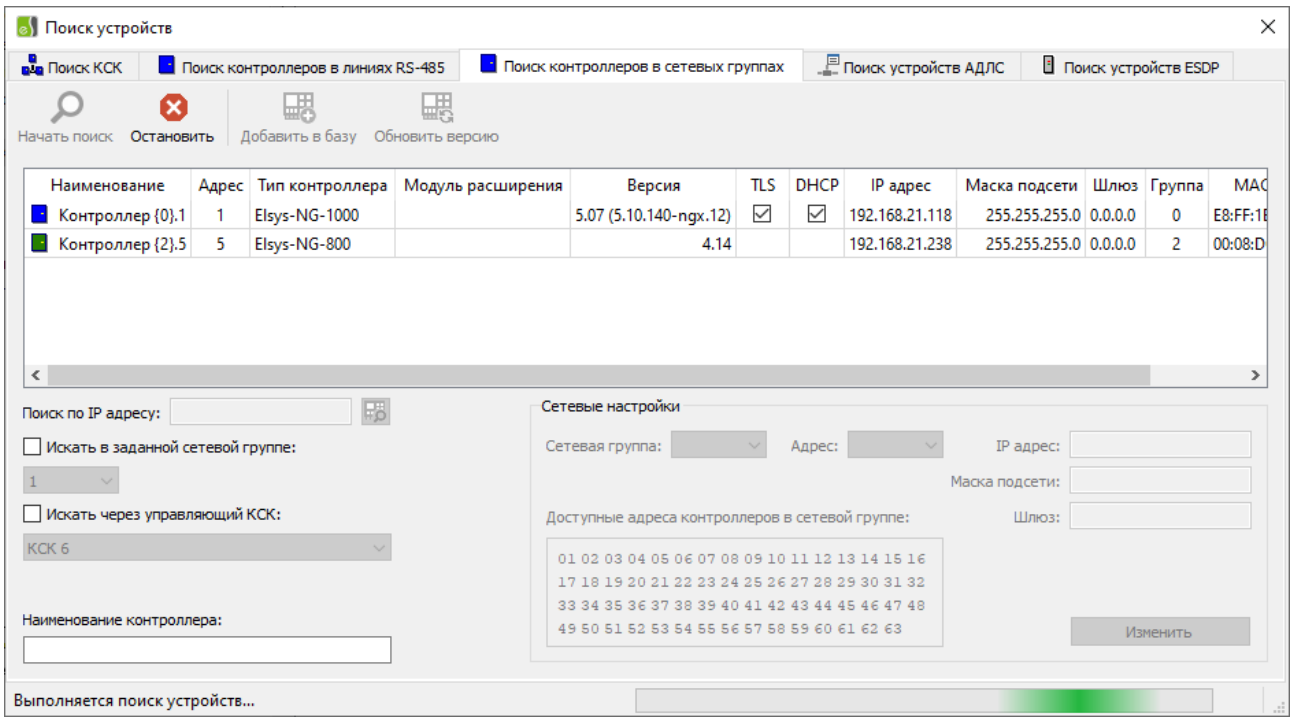

Рисунок 10. Окно формы поиска контроллеров с интерфейсом Ethernet

Информация о найденных контроллерах отображается в табличном виде. Адреса найденных контроллеров проверяются на совпадение с адресами контроллеров, уже существующих в конфигурации системы. При совпадении адресов перед условным наименованием контроллера в таблице отображается пиктограмма (существующий контроллер), при несовпадении – пиктограмма (новый контроллер). Для существующих контроллеров также выполняется дополнительная сверка версии, типа (варианта исполнения) и типа модуля расширения (для контроллеров доступа). Также сверяются сетевые параметры: IP адрес и маска подсети.

Контроллеры с настройками по умолчанию имеют IP-адрес 192.168.127.254 и номер сетевой группы равный нулю. Такие контроллеры запрещено добавлять в конфигурацию системы и их параметры должны быть настроены.

Настроить параметры как нового, так и существующего контроллера, можно непосредственно из окна поиска. Для этого необходимо выделить в таблице строку с информацией об изменяемом контроллере и указать нужные значения IP-адреса, маски подсети, адреса шлюза, номера сетевой группы и адреса контроллера в группе параметров «Сетевые настройки» внизу окна поиска и нажать кнопку «Изменить», после чего новые настройки будут

записаны в контроллер. Для удобства выбора в группе сетевых настроек размещена информационная панель «Доступные адреса контроллеров в сетевой группе». Свободные (доступные) адреса отображаются синим цветом, занятые – зеленым, красным цветом отображаются адреса контроллеров с конфликтом конфигурации. Если выбранный пользователем адрес контроллера конфликтует с адресом уже существующего в выбранной сетевой группе контроллера, то у пользователя будет запрошено подтверждение выполнения конфликтной операции. После смены настроек рекомендуется выполнить повторный поиск устройства для подтверждения изменений.

Если сетевая группа с номером, выбранным пользователем, не существует, то она будет создана в процессе выполнения процедуры изменения настроек контроллера как группа, опрашиваемая непосредственно сервером интеграции.

Внимание! Если у контроллера включен режим DHCP, то смена сетевых настроек, кроме сетевой группы, невозможна. Если включена опция TLS, то для установления соединения контроллер должен быть добавлен в защищённую сетевую группу, адрес должен быть установлен аппаратным способом, при этом настройка «Номер сетевой группы» роли не играет и может использоваться только для логического разделения устройств при поиске.

После изменения сетевых настроек выполняется повторная сверка информации о данном контроллере с информацией, записанной в конфигурации системы.

Поле формы «Наименование контроллера» для новых контроллеров заполняется автоматически генерируемым наименованием с возможностью ручного редактирования пользователем. Для существующих контроллеров условное наименование считывается из конфигурации системы и недоступно для редактирования пользователем.

После того как все настройки сделаны, новый контроллер может быть добавлен в конфигурацию системы кнопкой «Добавить в базу». Если для добавляемого контроллера существует хотя бы одна готовая конфигурация, то будет предложено выбрать готовую конфигурацию, совместимую с его типом

или вариантом исполнения. При отказе от выбора, либо при отсутствии готовой конфигурации, контроллер будет добавлен с пустой конфигурацией.

Для существующих контроллеров при конфликте версий можно выполнить процедуру обновления информации в конфигурации системы кнопкой «Обновить версию» после подтверждения запроса пользователем. При одновременном конфликте версий и конфигурации процедура обновления информации недоступна.

2.2.2.5 Поиск устройств АДЛС

Для поиска и конфигурирования устройств, подключенных к АДЛС охранного контроллера Elsys-AC2, необходимо выбрать вкладку «Поиск устройств АДЛС» (см. Рисунок 11). При нажатии расположенной на панели быстрого доступа формы кнопки «Начать поиск» запускается процедура поиска, фактически являющейся специальным сервисным режимом, в котором охранный контроллер непрерывно сканирует весь диапазон адресов и передаёт информацию о найденных расширителях. В этом режиме обеспечивается автоматический поиск устройств, подключенных в линию связи, чтение информации о них (тип прибора, версия встроенного программного обеспечения), и функционал изменения адреса и удаленного обновления прошивок адресных устройств. В отличие от других режимов поиска, которые завершаются автоматически, для завершения режима поиска устройств АДЛС обязательно нужно использовать команду остановки поиска, вызываемой по нажатию кнопки быстрого доступа «Остановить».

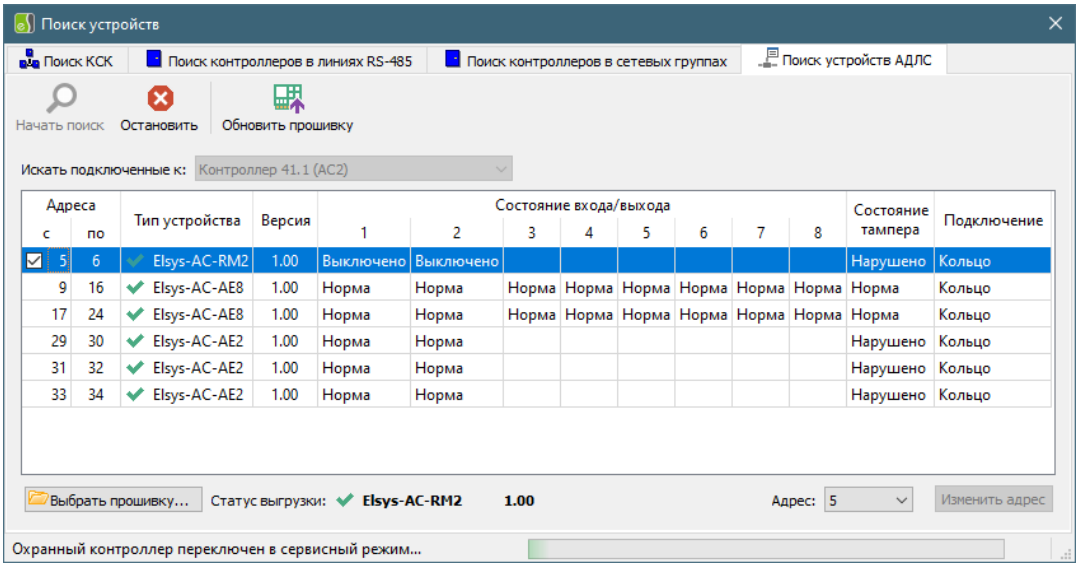

Рисунок 11. Окно формы поиска и конфигурирования устройств АДЛС

В процессе поиска выполняется группировка устройств по найденному типу и отображаются версия прошивки устройства, состояние входов (выходов) расширителя и тампера, а также способ подключения устройства к АДЛС. Если в процессе поиска выдаётся неполная информация об устройстве, то перед наименованием типа добавляется пиктограмма предупреждения ⚠. При совпадении всех адресов, обслуживаемых расширителем, с адресами устройств, сохраненными в конфигурации системы, перед именем типа добавляется пиктограмма соответствия конфигурации ✔. Информация по каждому найденному устройству при получении новых данных автоматически корректируется и группируется по типу.

Для обнаруженных устройств при отсутствии ошибок поиска доступна процедура смены адреса. Для запуска данной процедуры пользователь должен выбрать новый стартовый адрес расширителя АДЛС из выпадающего списка в нижней части вкладки поиска и нажать кнопку «Изменить адрес». Остальные адреса, принадлежащие выбранному расширителю, будут изменены автоматически. Процедура смены адреса может быть выполнена только в сервисном режиме работы охранного контроллера, т.е. только при запущённом режиме поиска. Устройство, для которого выполняется процедура смены адреса маркируется в таблице пиктограммой ожидания завершения процесса смены адреса 🕒.

Для активации возможности удаленного обновления прошивки необходимо выгрузить файл прошивки на сервер интеграции. Выгрузка может быть выполнена в любое время, независимо от запуска процесса поиска устройств. Статус выгрузки, тип устройства и версия прошивки отображаются в нижней части формы поиска. В таблице найденных устройств для расширителей, имеющих совместимый с загруженной прошивкой тип, в столбце стартового адреса отобразится поле выбора. Для запуска процесса удаленного обновления прошивок необходимо выбрать не менее одного устройства и нажать на панели быстрого доступа формы кнопку «Обновить прошивку».

Внимание! Функционал удаленного обновления прошивок устройств АДЛС доступен только для охранных контроллеров, имеющих версию прошивки не ниже 1.04.

После завершения поиска устройств АДЛС при наличии хотя бы одного корректно обнаруженного устройства пользователю будет предложено запустить процесс обновления конфигурации контроллера. При этом, для устройств, отсутствующих в конфигурации, будет выполнена операция добавления нового устройства, а для уже существующих – операция обновления параметров устройства. Если в процессе обновления конфигурации возникнут ошибки, то по завершению процесса обновления будет сформировано окно с сообщением о наличии ошибки и списком конфликтующих адресов устройств. Для корректно добавленных устройств в таблице будет отображена пиктограмма соответствия конфигурации. После обновления конфигурации контроллера будет выполнена загрузка обновленной конфигурации системы в сервер интеграции. Инициализация охранного контроллера должна быть выполнена пользователем самостоятельно в соответствии с описанием, приведённым в разделе 3.

2.2.2.6 Поиск устройств ESDP

Для поиска и конфигурирования устройств, подключенных к линиям связи ESDP, необходимо выбрать вкладку «Поиск устройств ESDP» (см. Рисунок 12). На этой вкладке доступны для выбора контроллеры, в которых включен интерфейс считывателей «ESDP» или «Защищённый ESDP». Перед началом поиска эти контроллеры должны быть проинициализированы.

В выпадающем списке «Линия связи» следует выбрать линию связи, для контроллеров которой будет выполняться поиск подключенных к ним устройств ESDP, а в выпадающем списке «Искать подключенные к..» выбрать конкретный контроллер или пункт «Все контроллеры».

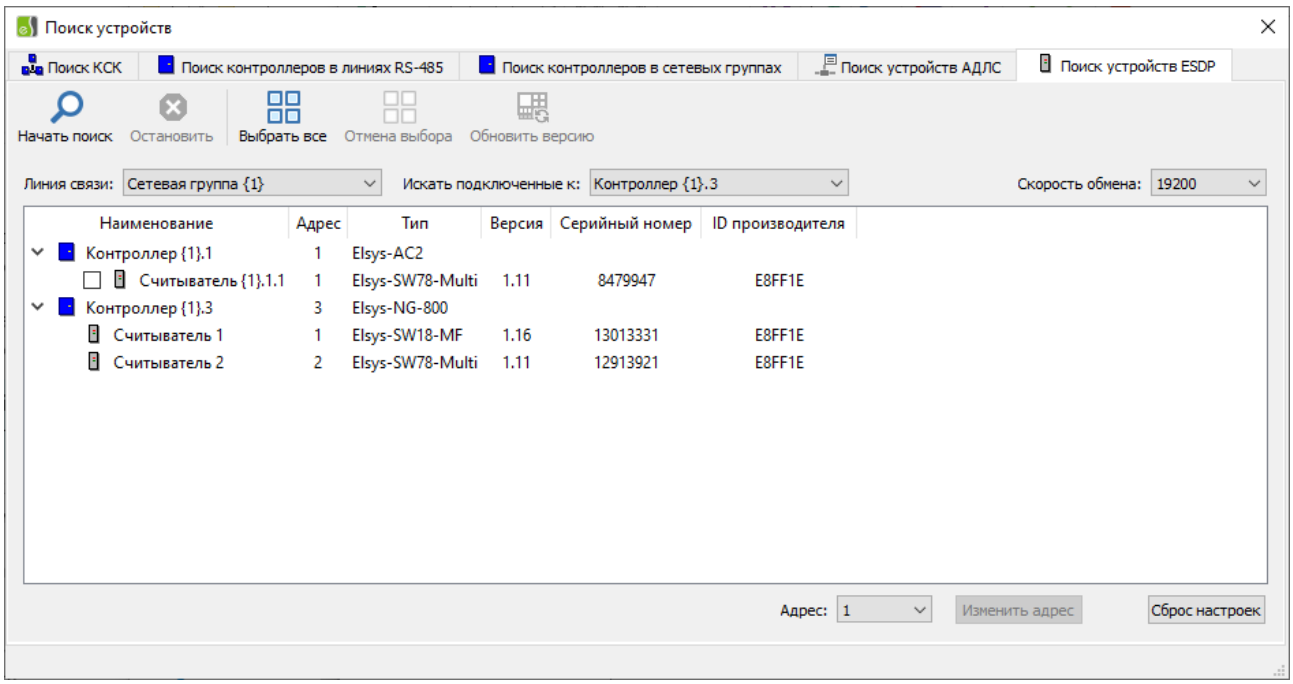

Рисунок 12. Окно формы поиска устройств ESDP

Если поле «Искать подключенные к..» имеет значение «Все контроллеры», то поиск будет выполняться в каждом контроллере на той скорости обмена, которая установлена в его конфигурации.

Если для поиска устройств ESDP выбран конкретный контроллер, в окне поиска становится доступным выпадающий список «Скорость обмена». Если выбранная скорость обмена отличается от указанной в конфигурации контроллера, будет произведена её смена для всех опрашиваемых устройств в начале поиска (на указанную в окне поиска) и для всех найденных устройств по окончании поиска (на скорость из конфигурации). Таким образом, скорость обмена найденных устройств ESDP по окончании поиска автоматически сменится на ту, что указана в конфигурации контроллера.

После установки параметров поиска для его запуска необходимо нажать кнопку «Начать поиск». Если в поле «Искать подключенные к..» выбран конкретный контроллер, поиск будет выполняться в диапазоне адресов 1 – 32, а если все контроллеры, то в диапазоне адресов 1 – 4.

Информация о найденных устройствах отображается в табличном виде. Найденные ESDP устройства отображаются в таблице как дочерние элементы контроллеров. В таблице выводятся наименование, адрес, тип прибора, версия встроенного программного обеспечения, серийный номер и ID производителя. Результаты обновляются в процессе поиска.

Процесс поиска завершается автоматически, либо может быть прерван по нажатию расположенной на панели быстрого доступа кнопки «Остановить».

После завершения поиска доступны: смена адреса, сброс настроек и обновление информации в конфигурации.

Для смены адреса необходимо выделить устройство, выбрать доступный адрес в нижнем левом углу и нажать «Изменить адрес».

Для сброса настроек необходимо выделить найденное устройство ESDP и нажать кнопку «Сброс настроек» в правом нижнем углу, при этом будет очищена вся конфигурация, кроме настроек адреса и скорости обмена ESDP.

Если устройство с найденным адресом присутствует в конфигурации, то для него доступно обновление типа и версии прошивки. Для этого необходимо установить соответствующую галочку в списке найденных устройств и нажать кнопку «Обновить версию», после чего в конфигурации обновится информация в соответствии с результатами поиска. Также можно выбрать сразу все доступные устройства для актуализации информации, если нажать кнопку «Выбрать все».

Оборудованием СКУД Elsys поддерживаются перечисленные ниже устройства с протоколом ESDP:

- считыватель Elsys-SW18-MF;
- считыватель Elsys-SW78-Multi;
- считыватель Elsys-SW78-KP-Multi.

Поиск устройств иного типа, подключенных к линиям связи ESDP (например, считывателей сторонних производителей), возможен, если эти устройства поддерживают команды запроса информации протокола OSDP. В этом случае конфигуратор не сможет определить тип устройства, а функции сброса настроек и обновления информации в конфигурации для него будут недоступны.

2.2.3 Настройка сетевых протоколов

Информация, приведённая в настоящей главе, распространяется на контроллеры доступа Elsys-NG-1000 и коммуникационные сетевые контроллеры Elsys-NG-Net II, а также совместимые с ними контроллеры и КСК.

2.2.3.1 Режим DHCP

Режим DHCP предназначен для подключения контроллеров в сеть Ethernet, где требуется использование динамических IP-адресов. В этом режиме контроллер получает сетевые настройки (IP-адрес, маска подсети, шлюз и др.) от DHCP сервера. Также в контроллерах с поддержкой DHCP доступен протокол EAP-TLS, который использует сертификаты для аутентификации в сети. Возможность работы протокола DHCP и способ его включения описаны в руководствах по эксплуатации на конкретные изделия.

Перед подключением контроллеров в сеть на сервере DHCP должны быть указаны соответствия между IP-адресами и MAC адресами (необходимо обратиться к системным администраторам). Наклейка с MAC адресом размещена на печатной плате устройства. Если необходима аутентификация по протоколу EAP-TLS, то в сети также должны быть сделаны соответствующие настройки, а в контроллере установлены целевые сертификаты (см. п. 2.2.3.5).

Режим DHCP целесообразно использовать совместно с режимом TLS, поэтому в контроллерах и КСК по умолчанию включен режим DHCP TLS. Для включения режима DHCP без TLS необходимо выполнить следующие шаги:

- включить режим DHCP (см. руководство по эксплуатации на конкретное изделие);
- с помощью утилиты FtpUpdateUtility выключить опцию DHCP TLS (см. п. 2.2.3.6).

Для профилирования сети помимо MAC адреса может использоваться hostname, который по умолчанию в контроллерах является уникальным и основанным на MAC-адресе (значение hostname по умолчанию приведено в руководстве по эксплуатации на конкретное изделие). Также предусмотрена возможность смены hostname (см. п. 2.2.3.7).

ВНИМАНИЕ! Не допускается использовать режим динамического получения IP-адреса в сети без настройки таблицы DHCP сервера. Перед подключением контроллера в сеть, необходимо заранее знать, какой IP-адрес ему будет назначен. Этот IP адрес не должен меняться в процессе штатной работы системы.

При использовании режима DHCP без TLS, перед добавлением контроллеров в конфигурацию, в окне поиска им необходимо задать сетевые параметры СКУД Elsys. Для КСК нужно установить номер (см. п. 2.2.2.2); для контроллеров доступа – адрес (если он не установлен аппаратным способом) и номер сетевой группы (см. п. 2.2.2.4). При смене настроек в контроллерах также будет установлен пароль системы.

2.2.3.2 Режим TLS

Режим TLS предназначен для установления защищённого соединения сервиса интеграции с контроллерами на основе взаимной проверки сертификатов по протоколу mTLS. Возможность поддержки режима TLS можно уточнить в руководстве на конкретное изделие. Сертификаты также используются для аутентификации в сети по протоколу EAP-TLS. Контроллеры поставляются с сертификатами по умолчанию, которые должны быть заменены.

Настройка режима TLS имеет две опции: «DHCP TLS» и «Static TLS». Если включена опция «DHCP TLS», режим TLS будет активен при включенном режиме DHCP. Если включена опция «Static TLS», режим TLS будет активен при выключенном режиме DHCP. По умолчанию опция «DHCP TLS» включена, а опция «Static TLS» выключена.

Для включения совместной работы режимов DHCP и TLS достаточно включить режим DHCP (см. руководство по эксплуатации на конкретное изделие).

Для включения режима TLS без DHCP необходимо выполнить следующие шаги:

- установить в контроллере режим статических сетевых настроек (см. руководство по эксплуатации на конкретное изделие);
- в окне поиска установить требуемый статический адрес;
- с помощью утилиты FtpUpdateUtility включить опцию Static TLS (см. п. 2.2.3.6).

В режиме TLS в контроллере доступа должен быть установлен адрес аппаратным способом. Для КСК дополнительных аппаратных настроек в режиме TLS не требуется. Номер сетевой группы для контроллера доступа и адрес (номер) для КСК для установления соединения не используются и предназначены только для логического разделения устройств.

Для подключения к КСК в режиме TLS необходимо в конфигурации в настройках коммуникационного контроллера включить опцию «Защищённый сетевой обмен» и указать FQDN или IP-адрес в поле «Доменное имя». При этом адрес (номер) может быть произвольным.

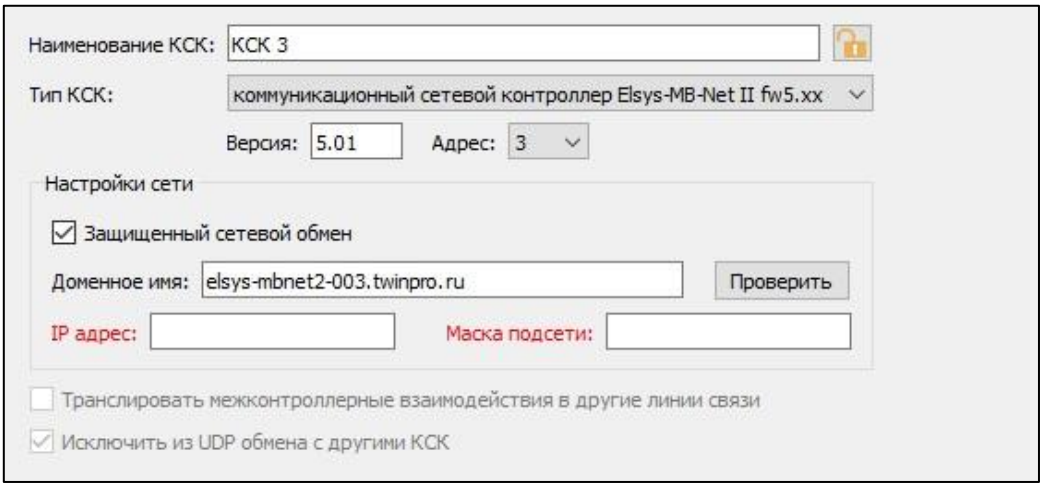

Рисунок 13. Настройка КСК для работы в режиме TLS

Для подключения к контроллеру доступа в режиме TLS, его необходимо добавить в «Защищённую сетевую группу» и указать в настройках адрес и FQDN или IP-адрес в поле «Доменное имя» (см. Рисунок 14). При этом номер сетевой группы может быть произвольным.

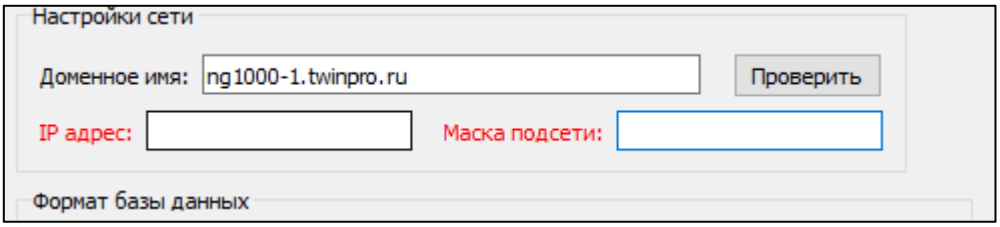

Рисунок 14. Настройка контроллера в защищённой сетевой группе

Установка соединения с контроллерами по протоколу mTLS может занимать несколько секунд.

2.2.3.3 Добавление устройств в режиме DHCP TLS в конфигурацию

В режиме DHCP TLS идентификация устройств должна происходить по соответствию значений FQDN/IP/MAC. MAC адрес является уникальным идентификатором контроллера в сети. Соответственно, в сетевой инфраструктуре должны быть настроены DHCP-сервер (для автоматического назначения IP-адреса и других сетевых настроек) и DNS-сервер (для возможности обращения к устройству по FQDN).

Чтобы добавить в конфигурацию устройства в режиме DHCP TLS, не требуется выполнение поиска. Для КСК достаточно знать FQDN или IP, а для контроллеров доступа, помимо этого, адрес, который выставляется аппаратным способом.

Для добавления КСК необходимо в дереве устройств вызвать контекстное меню правой кнопкой мыши на родительском элементе «Коммуникационный контроллеры» и выбрать требуемый тип. Далее нужно включить опцию «Защищённый сетевой обмен» для нового сетевого контроллера и указать FQDN или IP адрес в поле «Доменное имя», при этом адрес может быть произвольным.

Для добавления контроллера доступа нужно сначала добавить защищённую сетевую группу. Чтобы это сделать, необходимо правой кнопкой мыши вызвать контекстное меню на родительском элементе в дереве устройств «Сетевые группы», после чего выбрать пункт «Защищённая сетевая группа». Номер сетевой группы может быть произвольным. Для добавления контроллера в существующую сетевую группу необходимо нажатием правой кнопки мыши вызвать контекстное меню на соответствующем элементе в дереве устройств и выбрать тип. В новом контроллере в конфигурации необходимо указать адрес и FQDN или IP в поле «Доменное имя».

2.2.3.4 Подключение к контроллеру с помощью FtpUpdateUtility

Автономная утилита FtpUpdateUtility (см. Рисунок 15) предназначена для специфической настройки контроллеров с поддержкой режима TLS, а также для обновления прошивок. Утилита устанавливает соединение с контроллером только на момент выполнения требуемой функции.

В верхней части программы для подключения к контроллеру необходимо указать его IP-адрес или FQDN, порт подключения (см. в руководстве на конкретное изделие), пароль (по умолчанию admin) и сертификаты.

Утилита является клиентом по отношению к контроллеру. Для подключения к контроллеру с настройками по умолчанию необходимо использовать клиентские сертификаты, идущие в комплекте с FtpUpdateUtility.

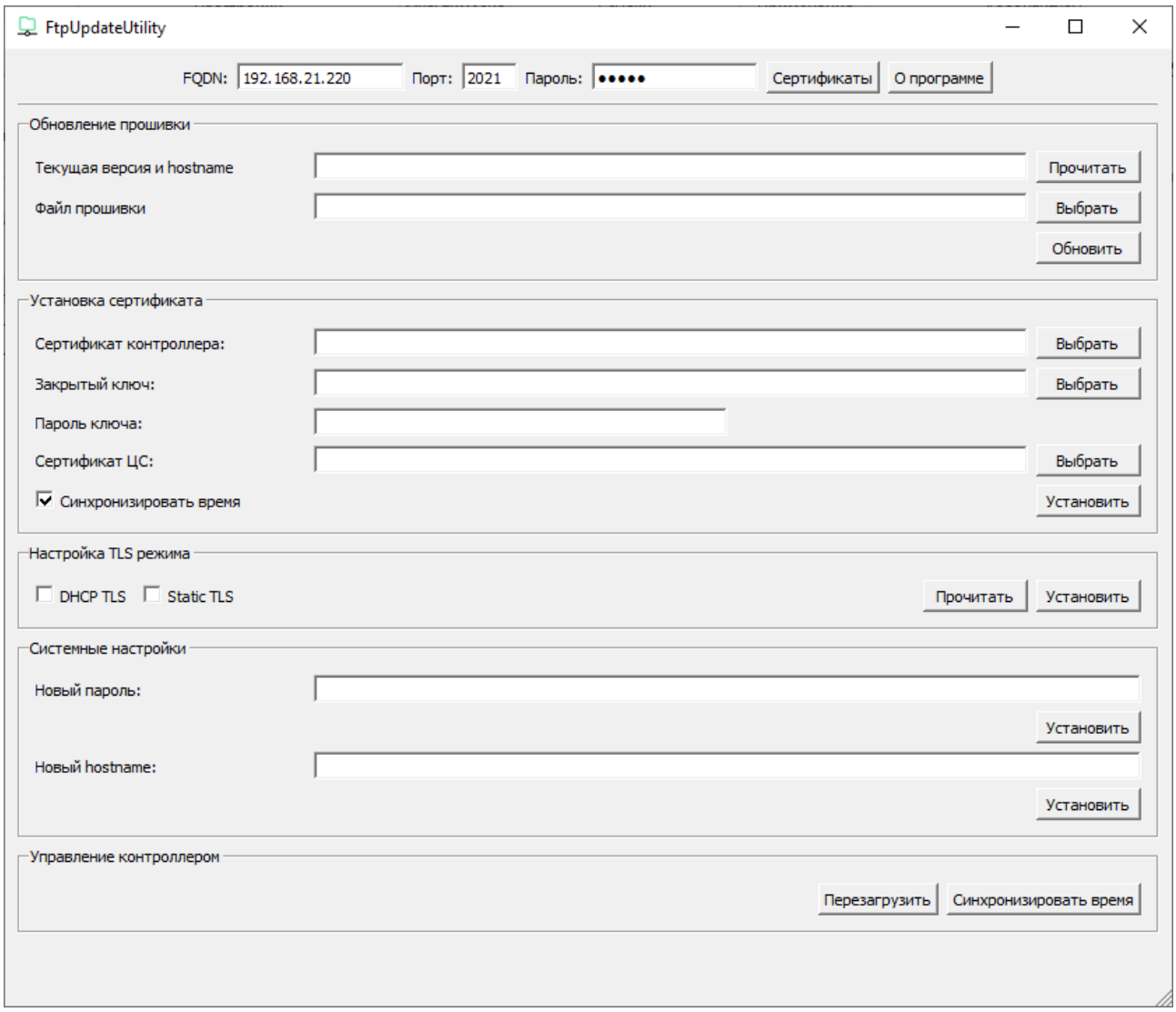

Рисунок 15. Окно утилиты FtpUpdateUtility

Чтобы указать сертификаты клиента (утилиты), необходимо нажать кнопку «Сертификаты» в верхней части экрана. В открывшемся окне (см. Рисунок 16) необходимо указать расположение файлов сертификата клиента, закрытого ключа и сертификата ЦС. Файлы должны быть в формате pem. Если закрытый ключ зашифрован с помощью пароля, то его необходимо указать в поле «Пароль ключа». Если указан IP адрес контроллера или FQDN, который не соответствует значению параметра «Common Name» в сертификате, загруженном в контроллер, то необходимо установить опцию «Не проверять имя сервера» (при подключении к контроллеру с настройками по умолчанию рекомендуется включить эту опцию). Файл «Сертификат ЦС» может содержать цепочку сертификатов. После завершения настройки сертификатов клиента, необходимо нажать кнопку «ОК».

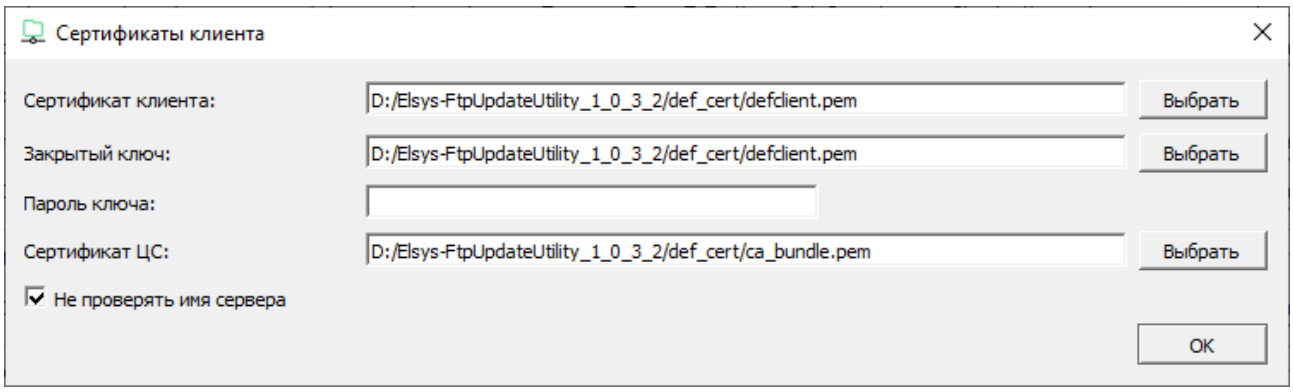

Рисунок 16. Настройка клиентских сертификатов

Чтобы проверить подключение, необходимо нажать кнопку «Прочитать» напротив поля «Текущая версия и hostname». В случае успешного подключения отобразится информация о контроллере (см. Рисунок 17). Где: «SKUD-Elsys-NG-1000-00-08-DC-2E-2D-31» – hostname контроллера; «5.10.140-ngx.12» – версия ядра; «Start time: 12:29:18 03.09.2024» – время старта прошивки по внутренним часам. Отображаемая информация может отличаться в зависимости от типа контроллера и его версии.

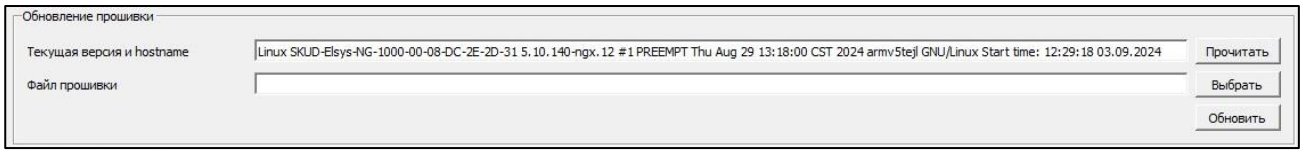

Рисунок 17. Информация о контроллере в утилите FtpUpdateUtility

2.2.3.5 Настройка сертификатов с помощью FtpUpdateUtility

Перед настройкой сертификатов необходимо убедиться, что удаётся успешно установить связь с контроллером (см. 2.2.3.4).

Целевые сертификаты сервера, которые необходимо загрузить в контроллер указываются в группе настроек «Установка сертификата» (см. Рисунок 18). Необходимо указать следующие файлы сертификат контроллера, закрытый ключ, сертификат ЦС. Файлы должны быть в формате pem. Если закрытый ключ зашифрован паролем, то его необходимо указать в поле «Пароль ключа». Для поля «Сертификат ЦС» можно указать несколько файлов с сертификатами, в том числе с цепочками, все сертификаты из выбранных файлов загрузятся в контроллер как доверенные. Опция «Синхронизировать время» включена по умолчанию. Она необходима для корректной работы контроллера после загрузки новых сертификатов, т.к. они могут иметь дату

начала действия позднее, чем время в контроллере по умолчанию. Чтобы запустить загрузку указанного сертификата, необходимо нажать на кнопку «Установить».

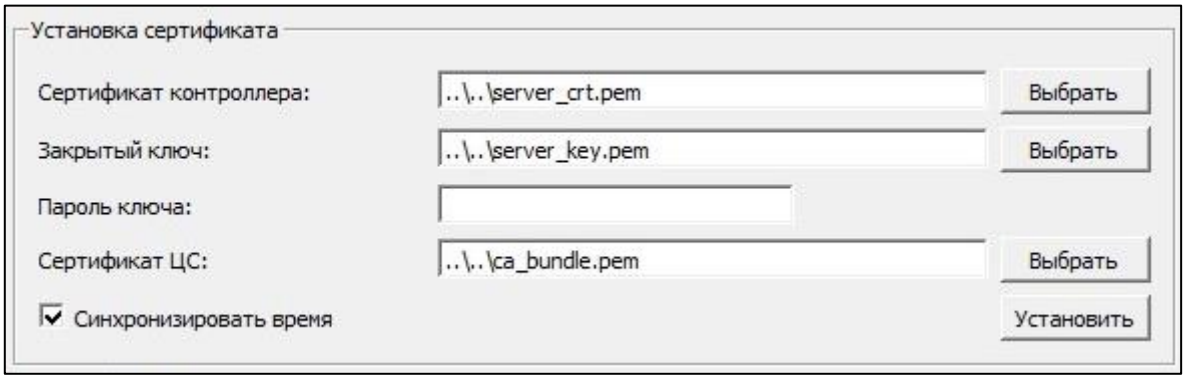

Рисунок 18. Настройка сертификатов сервера для загрузки

После загрузки проверьте установление соединения с указанием сертификата клиента, соответствующего сертификату сервера (см. 2.2.3.4).

2.2.3.6 Настройка TLS режима с помощью FtpUpdateUtility

Перед настройкой режима TLS необходимо убедиться, что удаётся успешно установить связь с контроллером (см. 2.2.3.4).

Текущие настройки TLS режима в контроллере можно прочитать, нажав кнопку «Прочитать» в группе настроек «Настройки TLS режима» (см. Рисунок 19). Результат также отобразится в этой группе.

Для включения требуемого режима TLS, необходимо установить соответствующую опцию в группе настроек «Настройка TLS режима», после чего нажать на кнопку «Установить».

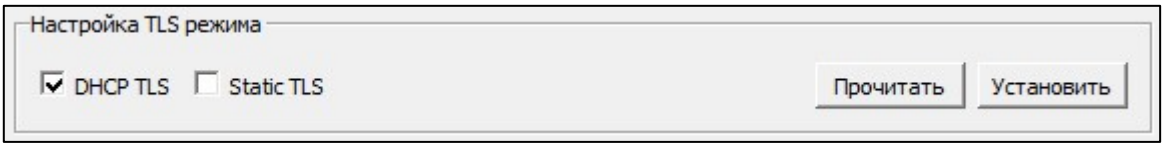

Рисунок 19. Настройка TLS режима

2.2.3.7 Смена системных настроек с помощью FtpUpdateUtility

Перед сменой системных настроек необходимо убедиться, что удаётся успешно установить связь с контроллером (см. 2.2.3.4).

К системным настройкам относятся следующие параметры: пароль доступа для утилиты FtpUpdateUtility и hostname контроллера. Для смены системной настройки необходимо в группе настроек «Системные настройки»

(см. Рисунок 20) ввести в поле требуемого параметра новое значение и нажать кнопку «Установить».

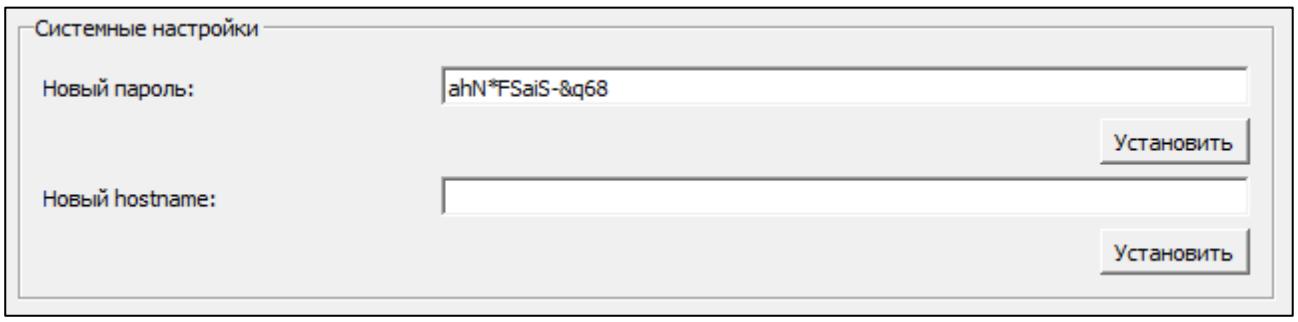

Рисунок 20. Системные настройки FtpUpdateUtility

2.2.3.8 Управление контроллером с помощью FtpUpdateUtility

Перед отправкой управляющей команды необходимо убедиться, что удаётся успешно установить связь с контроллером (см. 2.2.3.4).

Для отправки управляющей команды необходимо в группе «Управление контроллером» нажать на кнопку с требуемой функцией (см. Рисунок 21).

Рисунок 21. Управление контроллером с помощью FtpUpdateUtility

2.2.4 Настройка КСК

2.2.4.1 Добавление КСК в конфигурацию системы

Добавление КСК в конфигурацию системы может быть выполнено из окна поиска (см. п. 2.2.2.2) либо из контекстного меню узла «Коммуникационные контроллеры» в главном окне конфигуратора (см. Рисунок 22).

Если добавление КСК выполняется из контекстного меню конфигуратора, для самого КСК должны быть предварительно настроены сетевые параметры (IP-адрес, маска подсети, номер), а в окне настроек КСК эти параметры необходимо установить вручную. Пароль, установленный в КСК, должен совпадать с используемым в системе.

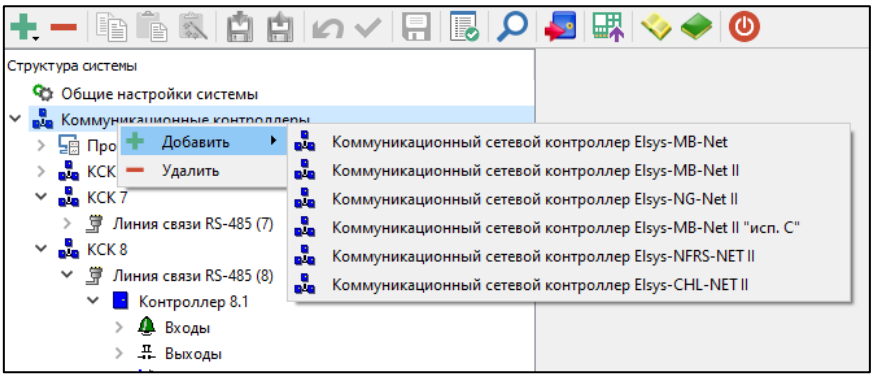

Рисунок 22. Добавление КСК в конфигурацию из контекстного меню

Если в КСК используются протоколы DHCP и TLS, его следует добавлять из контекстного меню, а для обмена информацией с ним достаточно задать его FQDN, а остальные сетевые параметры (IP-адрес, маска подсети, номер, пароль) роли не играют (см. п. 2.2.3.2, Рисунок 13).

2.2.4.2 Основные настройки КСК

При работе в составе СКУД Elsys КСК может выполнять две функции:

1) выступать в качестве контроллера, обеспечивающего опрос и управление контроллерами в сетевой группе и линии связи RS-485, обслуживаемыми этим КСК, а также обмен информацией с другими КСК;

2) выступать в качестве центрального контроллера охранной сигнализации, выполняя сбор и обработку информации от охранных контроллеров, и обеспечивая централизованное управление охранной сигнализацией для сегмента системы, состоящего из контроллеров, подключенных в линии связи этого КСК.

Окно настроек КСК (см. Рисунок 23) помимо информации о сетевых параметрах, присвоенных в окне поиска (IP-адрес, маска подсети, адрес), содержит перечисленные ниже данные.

«Наименование КСК» – текстовое поле, которое формируется автоматически и может быть изменено пользователем.

«Тип КСК» (соответствует аппаратному типу КСК) и «Версия» (версия встроенного программного обеспечения) – параметры, от которых зависит набор функциональных возможностей, алгоритм инициализации и обмена данными с КСК. Эти настройки обязательно должны соответствовать реальным. Возможные варианты для настройки *«Тип КСК»:*

– Elsys-MB-Net (имеют базовый функционал);
– Elsys-MB-Net II (обладают большей производительностью, по сравнению с Elsys-MB-Net; поддерживают функционал центрального контроллера охранной сигнализации);
– Elsys-NG-Net II (совместимы с Elsys-MB-Net II; поддерживают функционал центрального контроллера охранной сигнализации, сетевые протоколы DHCP, EAP-TLS, mTLS).

В случае, если при эксплуатации системы была выполнена замена КСК на другой тип, следует привести в соответствие с аппаратным типом настройку «тип КСК».

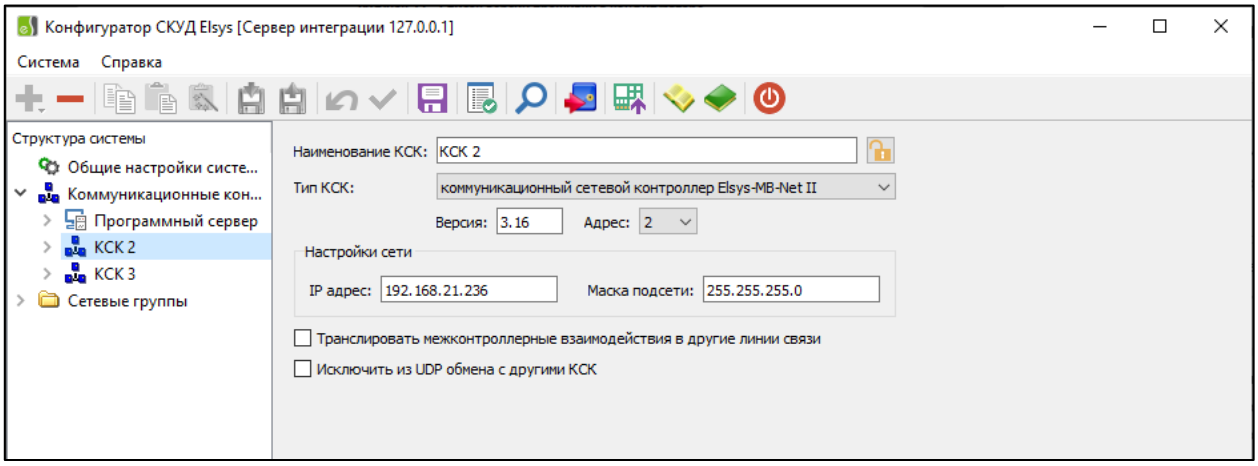

Рисунок 23. Окно настроек КСК

Опция «Транслировать межконтроллерные взаимодействия в другие линии связи», позволяет включать (отключать) передачу широковещательных сообщений от контроллеров доступа, подключенных к данному КСК, контроллерам, подключенных к другим КСК, что обеспечивает работу взаимодействий между контроллерами, находящимися в разных линиях связи RS-485 или сетевых группах;

Опцию «Исключить из UDP обмена с другими КСК» следует включать, если КСК не участвует в работе межконтроллерных взаимодействий или глобального аппаратного контроля последовательности прохода.

2.2.4.3 Настройка КСК для обслуживания линий связи СКУД Elsys

В дереве устройств узел «КСК» имеет дочерний узел «Линия связи RS-485». Если предполагается подключать устройства по линии RS-485,

необходимо настроить параметры линии связи (см. п. 2.2.5) и добавить в неё контроллеры из окна поиска согласно п. 2.2.2.3 или из контекстного меню.

Если требуется реализовать опрос устройств, подключаемых по интерфейсу Ethernet, необходимо добавить сетевую группу (см. п. 2.2.6), задав настраиваемый КСК в поле «КСК, осуществляющий опрос сетевой группы», после чего выполнить добавление контроллеров из окна поиска согласно п. 2.2.2.4 или из контекстного меню.

2.2.4.4 Настройка КСК для обслуживания охранной подсистемы

Для настройки охранной подсистемы предварительно требуется добавить КСК и устройства, которые предполагается использовать в качестве элементов охранной подсистемы.

Добавление конфигурации охранной подсистемы в конфигурацию КСК осуществляется нажатием кнопки ✚ на панели быстрого доступа при выбранном КСК в дереве устройств, либо из контекстного меню КСК.

После добавления конфигурации охранной подсистемы в КСК появится дочерний узел «Настройки охранной подсистемы» (см. Рисунок 24), включающий следующие настройки: «Локальные разделы», «Глобальные разделы», «Группы разделов», «Считыватели», «Управляющие выходы», «Пульты и модули индикации» и «Web-клиенты».

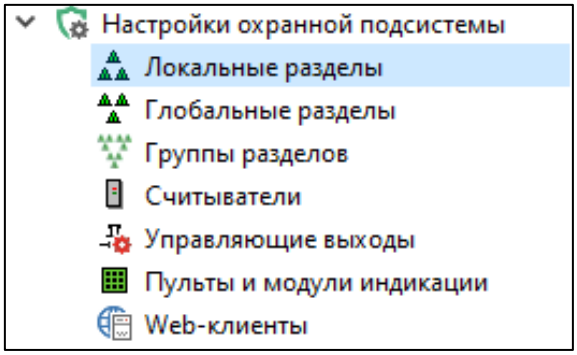

Рисунок 24. Отображение настроек
охранной подсистемы в дереве устройств

Назначение настроек охранной подсистемы:

– окно свойств узла «Локальные разделы» предназначено для добавления локальных разделов, заданных в конфигурациях контроллеров, опрашиваемых КСК для централизованного управления;

- окно свойств узла «Глобальные разделы» предназначено для конфигурирования глобальных разделов, в которые могут входить доступные входы, принадлежащие контроллерам, опрашиваемым КСК;
- окно свойств узла «Группы разделов» предназначено для задания разделов, объединённых пользователем в группы для совместного управления;
- окно свойств узла «Считыватели» служит для задания считывателям возможности управления разделами и группами, участвующими в централизованном управлении охраной;
- в окне свойств узла «Управляющие выходы» задаются выходы оповещения централизованной ОПС, программы их управления и список разделов, связанных с выходом управления;
- в окне свойств узла «Пульты и модули индикации» назначаются разделы или группы разделов для клавиатур Elsys-CP2, находящихся в режиме «Индикация и управление»;
- окно свойств узла «Web-клиенты» предназначено для настройки параметров сетевых рабочих мест, выполняющих информационное взаимодействие с КСК и разворачиваемых на любом сетевом устройстве (ПК, планшет, мобильное устройство и др.), на котором может быть запущен web-браузер.

Настройка централизованной охранной подсистемы описана в документе «ТСОС Elsys. Руководство по эксплуатации».

2.2.4.5 Настройка защищённого соединения TLS

Настройка КСК для работы в режиме защищённого TLS-соединения описана выше (см. п. 2.2.3.2, Рисунок 13).

2.2.5 Настройка линий связи RS-485

2.2.5.1 Основные настройки

Основные настройки, задающие режим обмена данными между контроллерами – «Скорость обмена» и «Режим обмена» (см. Рисунок 25).

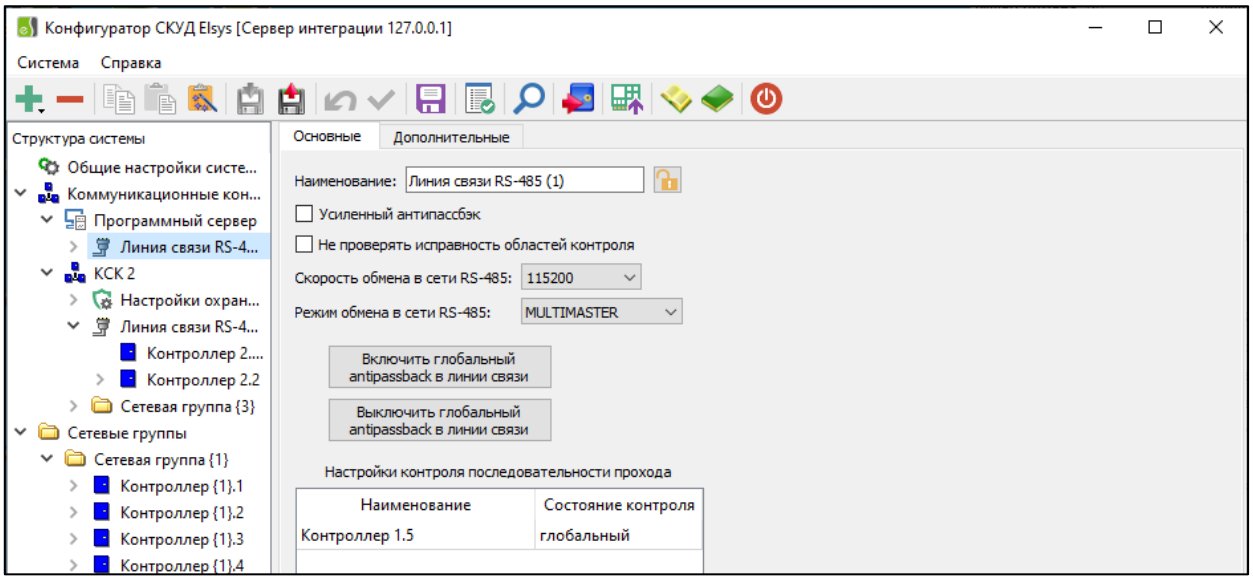

Рисунок 25. Окно формы настройки и конфигурирования линии RS-485

Настройка «Скорость обмена в сети RS-485» может принимать значения: 4800, 9600, 19200, 38400, 57600, 115200 бит/с (по умолчанию – 19200 бит/с). Скорость обмена всех контроллеров, подключенных в одну линию RS-485, должна соответствовать скорости, установленной в этой линии. Установку скорости обмена необходимо выполнять в соответствии с эксплуатационной документацией на оборудование.

Настройка «Режим обмена в сети RS-485» (возможные значения – MASTER-SLAVE или MULTIMASTER) задаёт режим обмена информацией между контроллерами и КСК. Режим MASTER-SLAVE используется при начальной настройке системы и может использоваться в дальнейшем, если обмен данными между контроллерами доступа осуществлять не требуется. Режим MULTIMASTER необходимо использовать, если необходимо организовать обмен информацией между контроллерами для осуществления функции «Глобальный контроль последовательности прохода» или для организации межконтроллерных взаимодействий.

Настройки «Усиленный antipassback» и «Не проверять исправность областей контроля» описаны ниже.

Линия связи RS-485 может быть подключена не только к КСК, но и к серверу интеграции, через преобразователь интерфейсов к USB или COM-порту компьютера. В этом случае необходимо указать номер COM-порта в

настройках сервиса интеграции. В остальном настройка идентична настройке линии RS-485, подключенной к КСК.

2.2.5.2 *Дополнительные настройки*

В окне дополнительных настроек (см. Рисунок 26) указаны параметры, предназначенные для настройки временных характеристик обмена информацией в линии связи. Изменения стандартных настроек может потребоваться при адаптации к сложным условиям эксплуатации линии RS-485. Без необходимости эти настройки изменять не следует. Для сброса настроек к значениям по умолчанию служит кнопка «Установить параметры по умолчанию».

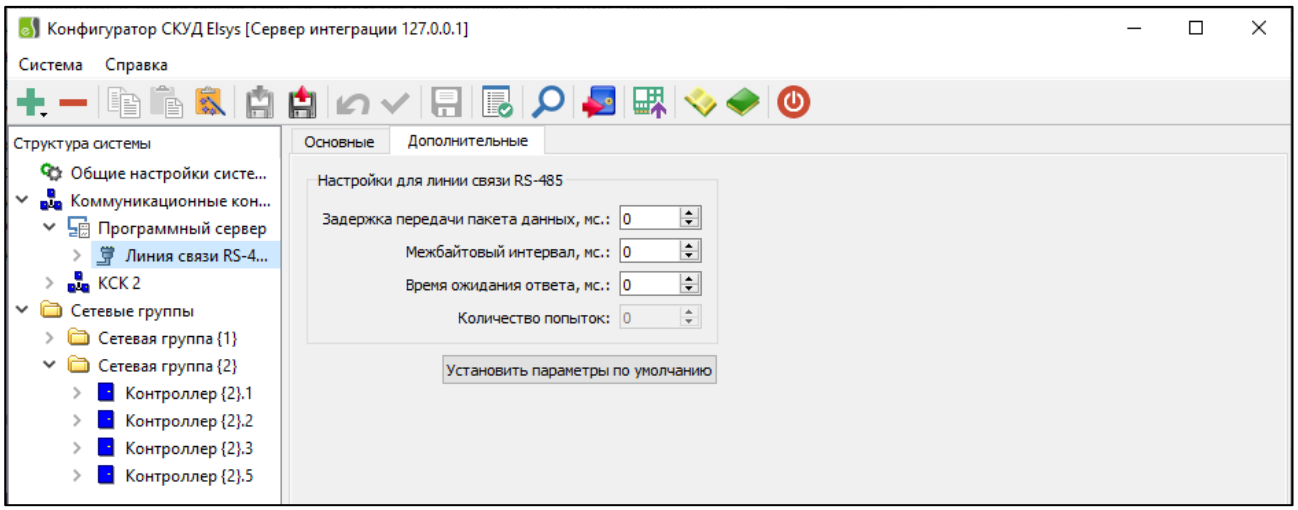

Рисунок 26. Окно формы дополнительных настроек линии RS-485

Настройка «Задержка передачи пакета данных» (0 – 127 мс, по умолчанию – 0) предназначена для формирования задержки очередной информационной посылки устройств, выполняющих обмен данными в линиях связи RS-485 сервера интеграции, КСК или контроллеров.

Настройка «Межбайтовый интервал» задаёт соответствующий таймаут для операции чтения, выполняемой КСК. В линии RS-485 сервера интеграции эта настройка не используется.

Настройка «Время ожидания ответа» задаёт для контроллеров линии связи таймаут ожидания ответа для операции чтения в режиме MULTIMASTER.

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

Если заданы нулевые значения, то значения для параметров «Время ожидания ответа» и «Межбайтовый интервал» автоматически устанавливаются внутренней логикой работы контроллеров и КСК в зависимости от скорости обмена, а количество попыток равно шести.

Дополнительные настройки линии связи загружаются в КСК автоматически, а в контроллеры линий связи – при инициализации.

Внимание! Для КСК версий 5.01 и выше, а также при условии наличия в линии связи хотя бы одного контроллера Elsys-NG-1000 автоматически устанавливаются задержка передачи пакета данных 1 мс, а время ожидания ответа – 100 мс. Для обеспечения надёжной работы информационного обмена эти параметры не следует изменять.

2.2.6 Настройка сетевых групп

Сетевая группа представляет собой логическое объединение контроллеров, поддерживающих IP-протоколы и физически подключаемых по интерфейсу Ethernet. Адресная ёмкость линии связи СКУД Elsys – 63 контроллера.

2.2.6.1 Добавление сетевых групп в конфигурацию системы

Добавление сетевых групп выполняется кнопкой ✚ на панели быстрого доступа либо в дереве устройств из контекстного меню КСК (см. Рисунок 27) или элемента «Сетевые группы» (см. Рисунок 28).

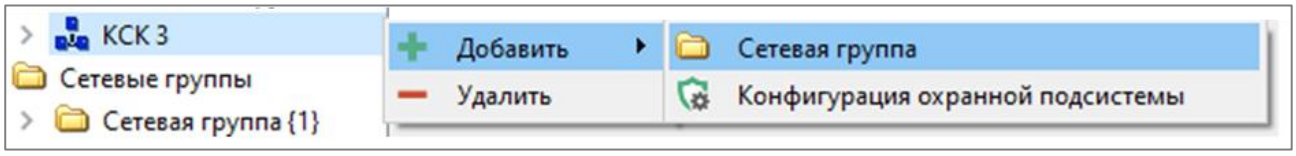

Рисунок 27. Добавление сетевой группы из контекстного меню КСК

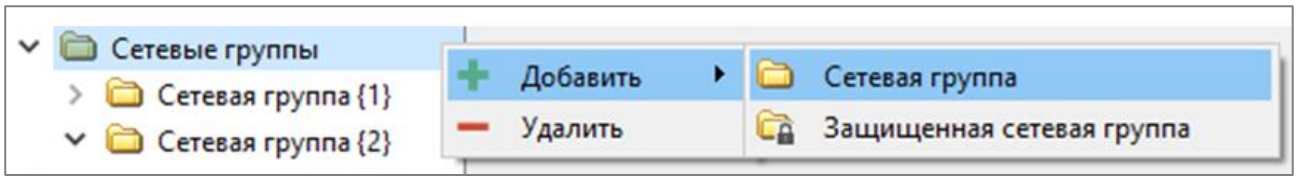

Рисунок 28. Добавление сетевой группы из контекстного меню сетевых групп

При добавлении присутствует возможность создать защищённую сетевую группу, в которую можно добавить только контроллеры Elsys-NG-1000 и совместимые с ними. Опрос контроллеров в составе защищённой сетевой группы может выполнять только сервер интеграции в режиме защищённого TLS-соединения. Обмен информацией между контроллерами, входящими в защищённую сетевую группу, невозможен.

2.2.6.2 Основные настройки

Окно настройки сетевой группы имеет вид, приведённый на рисунке (Рисунок 29).

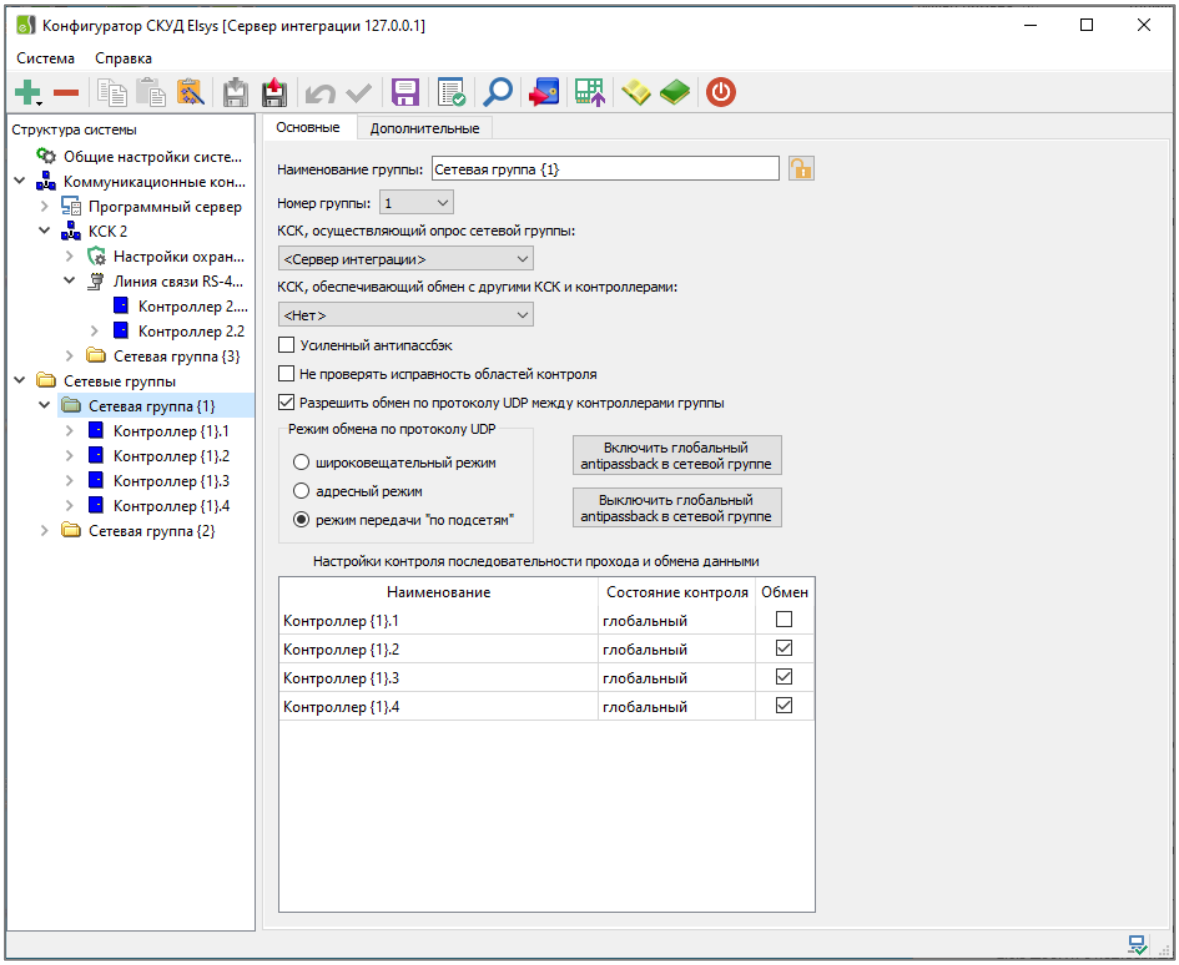

Рисунок 29. Окно настройки сетевой группы

Настройка «КСК, осуществляющий опрос сетевой группы» задаёт КСК, который выполняет сбор информации от устройств в выбранной сетевой группе. Если для опроса сетевой группы назначен КСК, она будет отображаться в дереве устройств как дочерний узел этого КСК, если не назначен – сетевая группа будет размещена в списке «Сетевые группы».

Настройка «КСК, обеспечивающий обмен с другими КСК и контроллерами» задаёт КСК, обеспечивающий организацию межконтроллерных взаимодействий и глобального контроля последовательности прохода.

Если требуется задать КСК для обеих указанных выше настроек, должен быть выбран один и тот же КСК.

Настройки «Усиленный antipassback» и «Не проверять исправность областей контроля» рассмотрены ниже.

2.2.7 Настройка обмена данными между КСК и контроллерами

Внимание! Обмен информацией между устройствами (КСК и контроллерами), подключенными к серверу интеграции в режиме защищённого TLS-соединения, невозможен.

2.2.7.1 Общие сведения

Для обеспечения аппаратных функций – глобального контроля последовательности прохода и межконтроллерных взаимодействий необходимо выполнить настройку обмена данными между оборудованием СКУД Elsys:

- между КСК (до 254 устройств);
- в линиях связи RS-485 всех КСК, участвующих в информационном обмене, путём включения режима MULTIMASTER (см. п. 2.2.5);
- в сетевых группах (до 63 контроллеров в группе).

Схема, иллюстрирующая взаимодействие оборудования СКУД Elsys, приведена на рисунке (Рисунок 3).

2.2.7.2 Настройка обмена данными между КСК

Настройка обмена данными между КСК выполняется в окне настройки общих параметров системы (см. Рисунок 5).

Настройки «Разрешить обмен по протоколу UDP всех КСК друг с другом», «Режим обмена по протоколу UDP» задают режим обмена

информацией по протоколу UDP между КСК. Эта настройка может принимать одно из трёх значений – «Широковещательный», «Адресный», «По подсетям». В первом случае при обмене информацией между КСК используются широковещательные пакеты (с IP-адресом получателя 255.255.255.255), во втором случае используются адресные пакеты, в третьем случае – пакеты с адресом подсети (например, 192.168.1.255).

Внимание! Для КСК, участвующих в информационном обмене, следует задавать адреса (номера) подряд, в порядке возрастания, без пропусков, начиная с 2 (адрес 1 обычно зарезервирован за сервером интеграции).

Если КСК не участвует в информационном обмене с другими КСК, следует в его настройках установить опцию «Исключить из UDP обмена с другими КСК».

2.2.7.3 Настройка обмена данными в сетевой группе

Настройка обмена данными между контроллерами сетевой группы выполняется в окне настройки параметров сетевой группы (см. Рисунок 29).

Если в системе несколько сетевых групп и/или линий связи и необходимо обеспечить обмен информацией с контроллерами из линий связи RS-485 и других сетевых групп, следует задать КСК в поле «КСК, обеспечивающий обмен с другими КСК и контроллерами».

Настройки «Разрешить обмен данными по протоколу UDP в сетевой группе», «Режим обмена по протоколу UDP» задают режим обмена информацией по протоколу UDP между контроллерами. Эта настройка может принимать одно из трёх значений – «Широковещательный», «Адресный», «По подсетям». В первом случае при обмене информацией между контроллерами используются широковещательные пакеты (с IP-адресом получателя 255.255.255.255), во втором случае используются адресные пакеты, в третьем случае – пакеты с адресом подсети (например, 192.168.1.255).

Внимание! Для контроллеров, участвующих в информационном обмене в сетевой группе, следует задавать адреса подряд, в порядке возрастания, без пропусков, начиная с 1.

Если контроллер не участвует в информационном обмене, следует в его настройках установить опцию «Исключить из UDP обмена с другими контроллерами».

2.2.7.4 Дополнительные настройки

Дополнительные параметры информационного обмена для КСК настраиваются на вкладке «Дополнительные» узла «Общие настройки системы» (см. Рисунок 30).

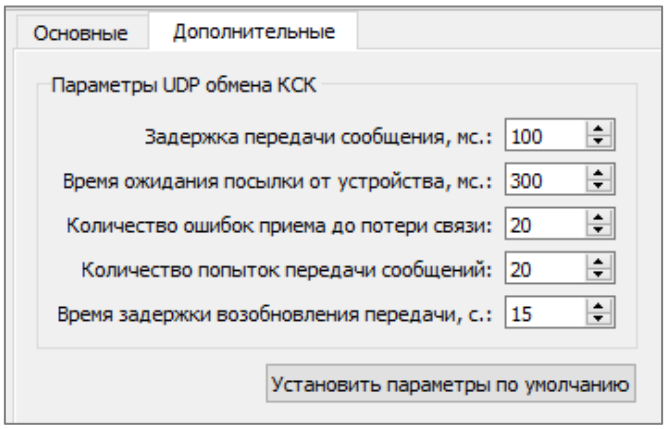

Рисунок 30. Окно дополнительных настроек системы

Дополнительные параметры UDP-обмена для сетевых групп настраиваются аналогично КСК, они размещены на вкладке «Дополнительные» узла «Сетевая группа». Без необходимости эти настройки изменять не следует. Для сброса настроек к значениям по умолчанию служит кнопка «Установить параметры по умолчанию».

При большом количестве устройств для уменьшения длительности цикла информационного обмена между КСК или контроллерами рекомендуется уменьшить значение параметра «Задержка передачи сообщения» до 15 мс.

2.2.8 Настройка контроллеров

2.2.8.1 Добавление контроллеров в конфигурацию системы.

Добавление контроллера в конфигурацию системы может быть выполнено из окна поиска (см. п. 2.2.2.3, 2.2.2.4) либо из контекстного меню узла линии связи RS-485 или сетевой группы (см. Рисунок 31).

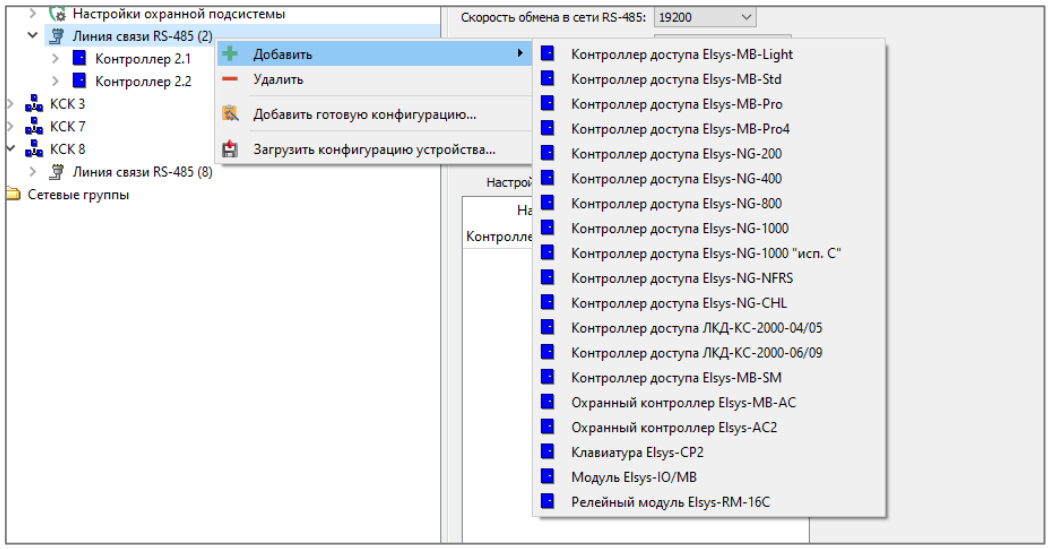

Рисунок 31. Добавление контроллера в конфигурацию
из контекстного меню

Если добавление контроллера выполняется из контекстного меню сетевой группы, для него должны быть предварительно настроены сетевые параметры (IP-адрес, маска подсети, номер сетевой группы, адрес), а в окне настроек контроллера эти параметры необходимо установить вручную. Пароль, установленный в контроллере, должен совпадать с используемым в системе.

Если в контроллере используются протоколы DHCP и TLS, его следует добавлять из контекстного меню защищённой сетевой группы, а для обмена информацией с ним достаточно задать его FQDN и адрес, а остальные сетевые параметры (IP-адрес, маска подсети, номер сетевой группы, пароль) роли не играют.

При дальнейшей настройке оборудования следует либо использовать готовые конфигурации (см. п. 2.2.8.2) либо самостоятельно выполнять добавление и настройку дочерних устройств контроллера. Настоятельно рекомендуется использовать готовые конфигурации, представляющие собой заранее настроенные наборы параметров контроллера и его дочерних устройств (точки доступа, считыватели, входы, выходы, взаимодействия, логические формулы и т. п.). В дальнейшем при необходимости может быть выполнена дополнительная настройка конфигурации.

2.2.8.2 Использование готовых конфигураций контроллеров

Выбрать готовую конфигурацию можно при добавлении контроллера из окна поиска (см. п. 2.2.2.3, 2.2.2.4), из контекстного меню линии связи или

сетевой группы (см. Рисунок 31, пункт «Добавить готовую конфигурацию..»), либо из контекстного меню устройства (см. Рисунок 32, пункт «Заменить готовой конфигурацией…»).

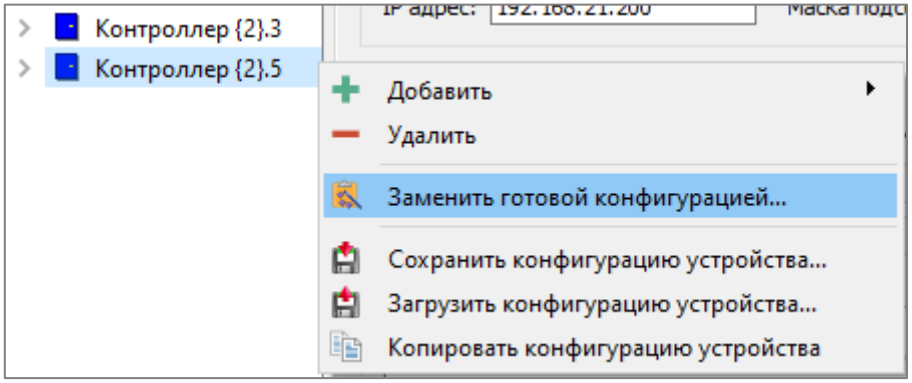

Рисунок 32. Выбор готовой конфигурации из контекстного меню

В открывшемся окне (см. Рисунок 33) будут отображены все конфигурации, которые доступны для настраиваемого контроллера в соответствии с его типом (вариантом исполнения). При добавлении из контекстного меню линии связи или сетевой группы вариант исполнения может быть выбран в соответствующем выпадающем списке.

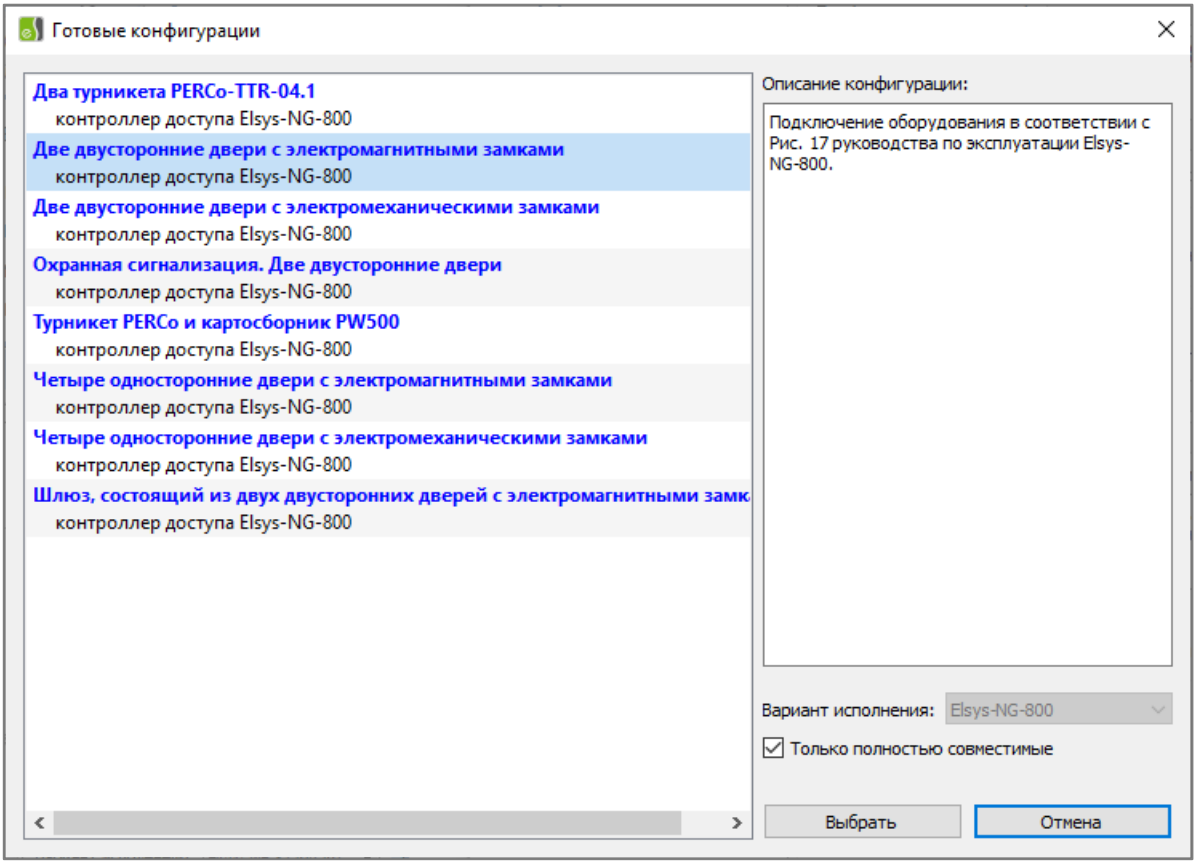

Рисунок 33. Окно выбора готовой конфигурации

Также в поле «Описание конфигурации» будет отображена краткая информация о выбранной конфигурации, и ссылка на документ, в котором приведена схема подключения периферийных устройств для корректной работы конкретной конфигурации.

Выбранная опция «Только полностью совместимые» отображает конфигурации, созданные для конкретного контроллера. При выключении опции будут отображаться конфигурации, которые могут потребовать внесения дополнительных доработок в конфигураторе для настройки совместимости в соответствии с аппаратными возможностями применяемого контроллера.

Кнопка «Выбрать» применяет конфигурацию, которая на данный момент активна, кнопка «Отмена» закрывает окно без внесения изменений.

После выбора конфигурации контроллера требуется сохранить изменения и выполнить инициализацию оборудования.

Конфигуратор поддерживает копирование (см. Рисунок 34) и вставку (см. Рисунок 35) конфигураций контроллеров. Для копирования конфигурации контроллера необходимо выбрать контроллер в дереве устройств, содержащий конфигурацию, которая будет скопирована, и вызвать контекстное меню, в котором выбрать пункт «Копировать конфигурацию устройства».

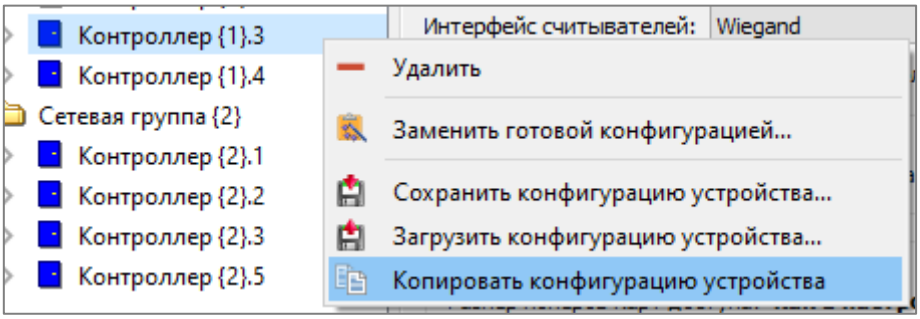

Рисунок 34. Копирование конфигурации устройства

Скопированную конфигурацию можно вставить в сетевую группу или линию связи RS-485, а также заменить конфигурацию существующего контроллера, используя контекстное меню, в котором следует выбрать пункт «Вставить копию <имя контроллера, чья конфигурация была скопирована>». При вставке конфигурации появится окно с предупреждением удаления старой

конфигурации. При несовпадении типов существующего и загружаемого контроллеров появится окно с сообщением об ошибке.

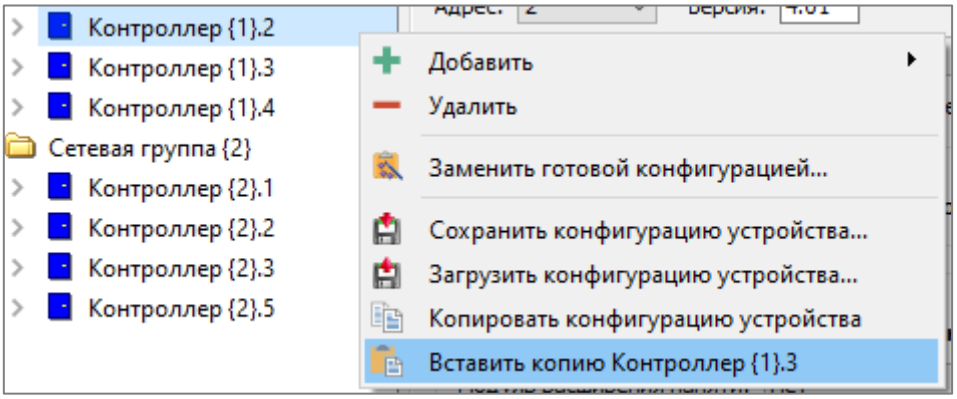

Рисунок 35. Вставка скопированной конфигурации

2.2.8.3 Основные настройки контроллеров

Основные настройки контроллеров размещены на вкладке «Основные» окна свойств контроллера (см. Рисунок 36).

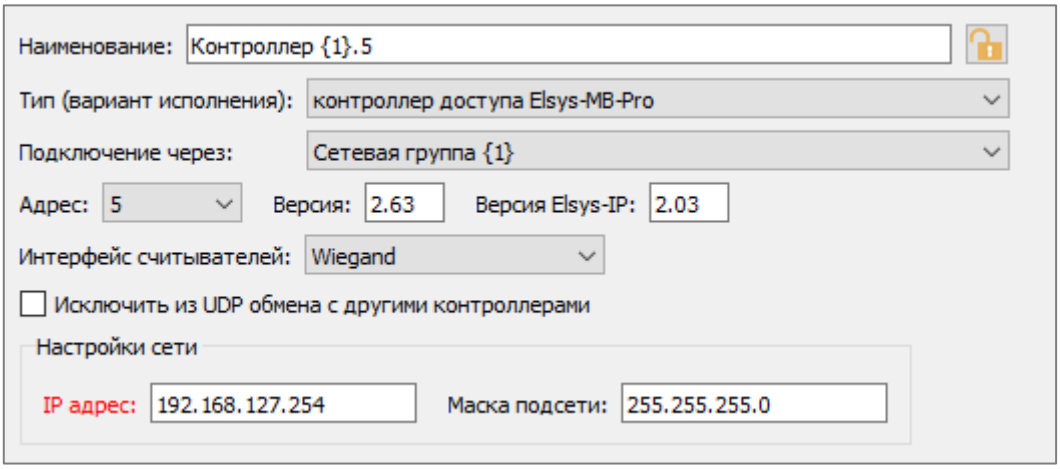

Рисунок 36. Основные настройки контроллеров

Назначение основных настроек описано ниже.

«Наименование» – текстовое поле, которое формируется автоматически и может быть изменено пользователем.

«Тип (вариант исполнения)» – настройка устанавливается автоматически при добавлении контроллера. Для совместимых типов контроллеров возможна смена типа на другой в выпадающем списке.

«Адрес» и «Версия» задают одноименные настройки контроллера.

«Версия Elsys-IP» (только для контроллеров Elsys-MB, подключаемых в сеть Ethernet) – версия прошивки модуля Elsys-IP.

«IP-адрес», «Маска подсети» – настройки IP-протокола, необходимые для подключения контроллера в сеть Ethernet. Эти настройки недоступны при подключении контроллера в линию связи RS-485.

«Интерфейс считывателей» задаёт интерфейс подключения для считывателей, обслуживаемых контроллером.

В зависимости от типа контроллера возможны следующие интерфейсы подключения считывателей:

– «Wiegand»;
– «Touch Memory»;
– «Защищённый Wiegand»;
– «ESDP»;
– «Защищённый ESDP».

«Подключение через» – поле для установки сетевой группы или линии связи RS-485, в которую подключен контроллер. Значение настройки устанавливается автоматически после добавления контроллера и может быть изменено пользователем, если при переконфигурировании системы необходимо переместить контроллер в другую линию связи.

«Исключить из UDP обмена с другими контроллерами» – настройка описана в п. 2.2.7.3.

Особенности настройки контроллеров доступа и охранных контроллеров приведены в п. 2.2.8.4 – 2.2.8.8.

2.2.8.4 Настройка контроллеров Elsys-MB (Pro, Std, Light, Pro4)

Первоначальная настройка выполняется согласно п. 2.2.8.1, 2.2.8.2.

На вкладке основных настроек (см. Рисунок 37) контроллеров Elsys-MB размещена группа настроек «Формат базы данных», используемая для задания распределения памяти контроллера между числом карт, временных интервалов, элементов уровней доступа и числом событий. Назначение параметров этой группы настроек описано ниже.

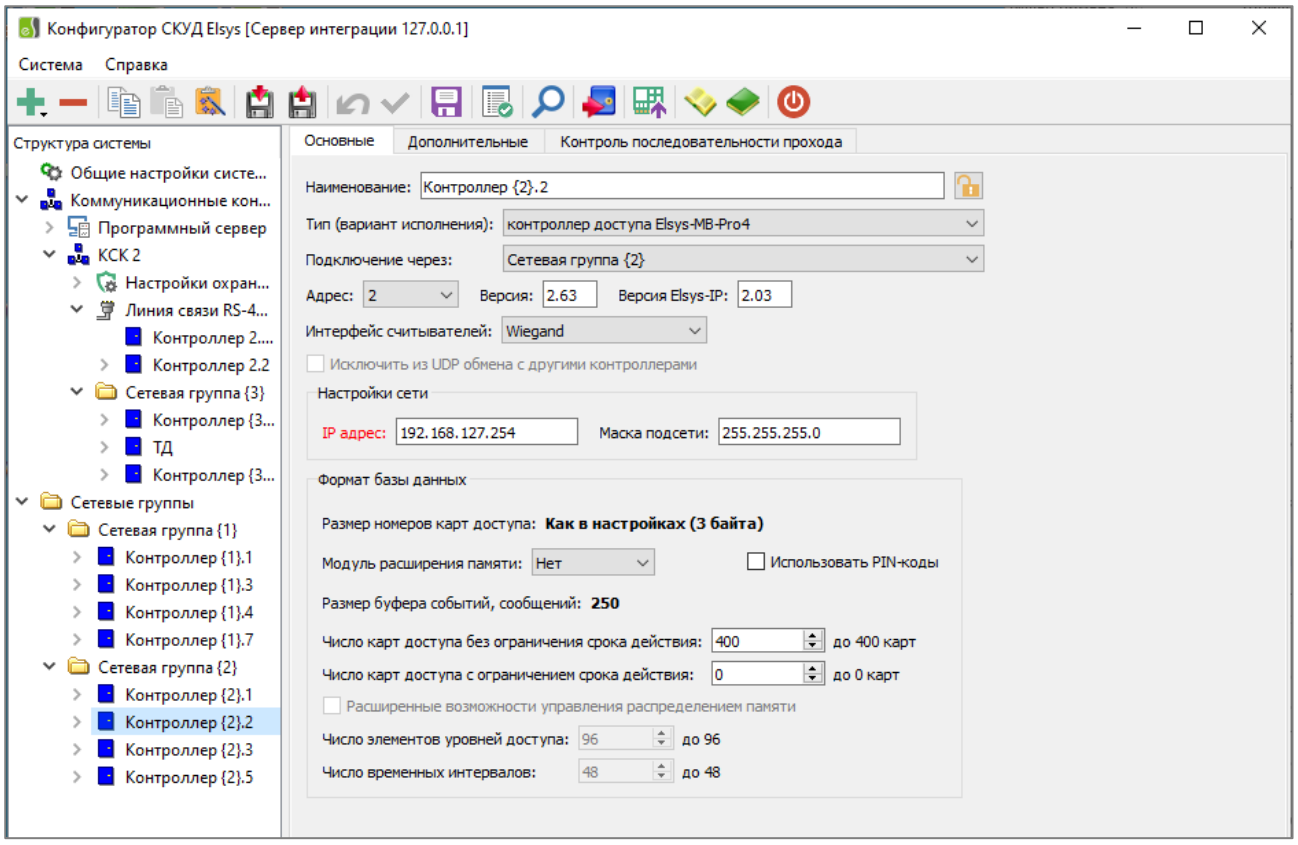

Рисунок 37. Основные настройки контроллеров Elsys-MB

«Модуль расширения памяти» – опция, определяющая тип или наличие модуля расширения памяти. Возможные значения – «Нет», «Elsys-XB2», «Elsys-XB8», «Elsys-XB32», «Elsys-XB64», «Elsys-XB128». Если модуль памяти установлен, то его тип в настройках контроллера должен соответствовать фактическому, отображаемому в окне поиска (см. п. 2.2.1).

«Размер номеров карт доступа» – параметр, отображающий размер номеров карт доступа в контроллере и не доступный для редактирования. Размер номеров карт в контроллере устанавливается автоматически в соответствии с одноимённым параметром в общих настройках системы. Если заданный размер номеров карт в контроллере не поддерживается, то название параметра будет отображаться красным цветом.

«Число карт доступа без ограничения срока действия» – параметр, задающий максимальное количество постоянных карт в памяти контроллера.

«Число карт доступа с ограничением срока действия» – параметр, задающий максимальное количество временных и разовых карт в памяти контроллера.

«Использовать PIN-коды» – опция, обеспечивающая возможность использования PIN-кодов в качестве дополнительного или основного идентификационного признака.

«Расширенные возможности настройки» (доступен при наличии модуля расширения памяти) – параметр, позволяющий задавать число элементов уровней доступа и временных блоков (см. соответствующие настройки, описанные ниже). Кроме того, включение этой опции обеспечивает следующие возможности:

- временной контроль последовательности прохода;
- подсчёт персонала;
- расширение диапазона значений номеров уровней доступа и временных блоков до 16382 (если эта опция выключена, диапазон номеров уровней доступа и временных блоков составляет 1 – 1022).

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

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

На вкладке дополнительных настроек (см. Рисунок 38) доступны опции «Параметры ввода PIN-кода», «Не реагировать на предъявление одной карты в течение…», «Использовать тампер», «Использовать мониторинг питания», «Мониторинг сигнала «Аккумулятор разряжен», «Устанавливать устройства после сброса в исходное состояние».

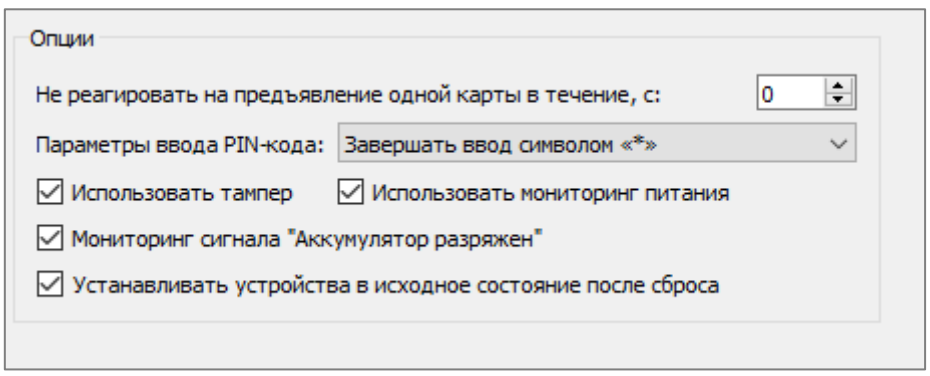

Рисунок 38. Дополнительные настройки контроллеров Elsys-MB

Опция «Параметры ввода PIN-кода» определяет, каким символом завершается ввод PIN-кода. Возможные значения – «Завершать ввод PIN-кода символом *» (по умолчанию) и «Завершать ввод PIN-кода символом # (как в N-1000)».

«Не реагировать на предъявление одной карты в течение …» – опция, обеспечивающая отсутствие реакции на повторное предъявление карты любому считывателю контроллера в течение заданного времени (диапазон значений 0-127 с). Опция может использоваться при настройке усиленных алгоритмов доступа.

При включенной опции «Использовать тампер» вход 20 используется для подключения датчика вскрытия корпуса.

При включенной опции «Использовать мониторинг питания» вход 21 используется для подключения сигнала «Авария сетевого питания».

При включенной опции «Мониторинг сигнала «Аккумулятор разряжен» вход 15 используется для подключения сигнала «Аккумулятор разряжен».

Если соответствующие опции выключены, входы 15, 20, 21 могут использоваться как цифровые входы общего назначения.

При выбранной опции «Устанавливать устройства после сброса в исходное состояние» после выполнения программного или аппаратного сброса все устройства переходят в исходное состояние, иначе все состояния остаются теми, что и были до сброса.

Описание настроек вкладки «Контроль последовательности прохода» приведено в п. 2.3.

2.2.8.5 *Настройка контроллеров Elsys-NG-xx*

Настоящая глава распространяется на контроллеры доступа Elsys-NG-200, Elsys-NG-800, Elsys-NG-1000 (далее – Elsys-NG-xx).

Первоначальная настройка выполняется согласно п. 2.2.8.1, 2.2.8.2.

На вкладке основных настроек (см. Рисунок 39) размещена группа настроек «Формат базы данных». Назначение параметров этой группы настроек описано ниже.

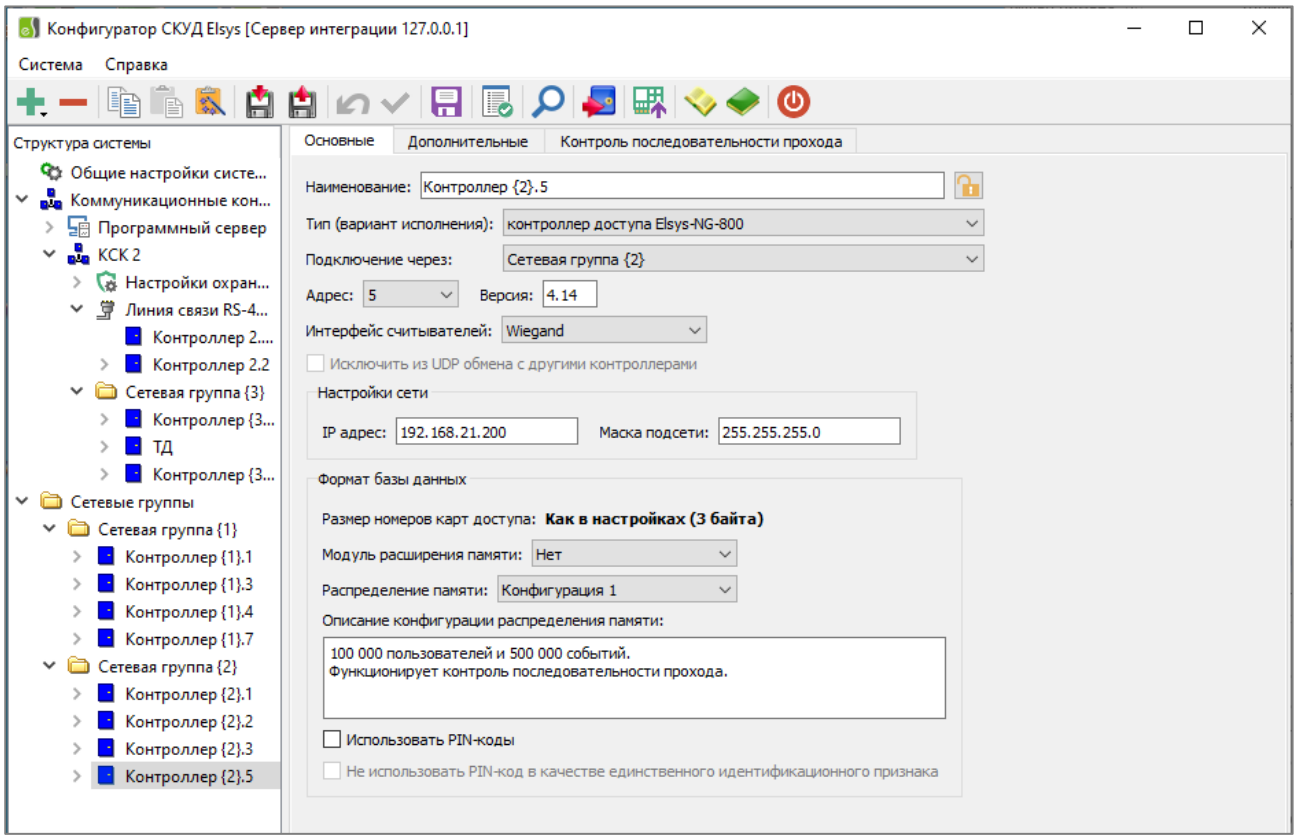

Рисунок 39. Основные настройки контроллеров серии Elsys-NG-xx

«Размер номеров карт доступа» – параметр, отображающий размер номеров карт доступа в контроллере, не доступен для редактирования. Назначение опции соответствует описанию аналогичной опции для контроллеров Elsys-MB (см. п. 2.2.8.4).

Опция «Распределение памяти» (используется только для Elsys-NG-800) обеспечивает выбор одной из трёх заранее настроенных моделей распределения памяти между картами и событиями (описание выбранной конфигурации отображается в поле «Описание конфигурации распределения памяти»).

«Использовать PIN-коды» – опция, обеспечивающая возможность использования PIN-кодов в качестве дополнительного или основного идентификационного признака.

Опция «Не использовать PIN-код в качестве единственного идентификатора» отключает возможность использования PIN-кода в качестве основного идентификационного признака. Включение этой опции ускоряет работу контроллера при анализе вводимых идентификационных признаков – контроллер будет проверять введённый PIN-код только на соответствие предъявленной карте, не выполняя поиск введённого PIN-кода во внутренней базе данных.

На вкладке дополнительных настроек (см. Рисунок 40) доступны опции «Параметры ввода PIN-кода», «Не реагировать на предъявление одной карты в течение…», «Использовать тампер», «Инверсный сигнал «Авария сетевого питания», «Устанавливать устройства после сброса в исходное состояние».

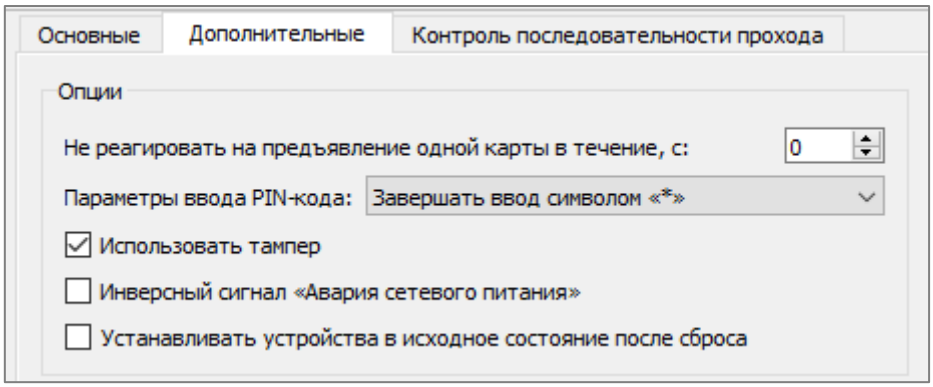

Рисунок 40. Дополнительные настройки контроллеров серии Elsys-NG-xx

Назначение настроек «Параметры ввода PIN-кода», «Не реагировать на предъявление одной карты в течение…», «Использовать тампер», «Устанавливать устройства после сброса в исходное состояние» соответствует описанию, данному в п. 2.2.8.4.

Настройка «Инверсный сигнал «Авария сетевого питания», обеспечивает поддержку источников питания с инверсным сигналом «Авария сетевого питания». (Если опция включена – нормальное состояние входа «Замкнуто», если выключена – «Разомкнуто»). Для версий прошивок, не поддерживающих эту функцию, настройка недоступна.

Настройка «Устанавливать устройства после сброса в исходное состояние» для контроллеров Elsys-NG-200 недоступна (в Elsys-NG-200 после выполнения сброса всегда выполняется установка устройств в исходное состояние).

При настройке Elsys-NG-1000 и совместимых с ним контроллеров в защищённой сетевой группе требуется настроить у контроллеров защищённый режим и заполнить дополнительное поле сетевых настроек «Доменное имя» (см. Рисунок 14). Подробная настройка описана в п. 2.2.3.2.

2.2.8.6 Настройка контроллеров серии ЛКД-КС-2000

Настоящий раздел распространяется на контроллеры ЛКД-КС-2000-02/03, ЛКД-КС-2000-04/05, ЛКД-КС-20-06/09.

Первоначальная настройка выполняется согласно п. 2.2.8.1, 2.2.8.2.

Для контроллеров данного типа предусмотрено использование только готовых конфигураций.

Настройка свойств контроллера выполняется аналогично настройке свойств контроллеров Elsys-NG-xx (см. п. 2.2.8.5).

После добавления в базу для контроллеров ЛКД-КС-2000 доступны возможности редактирования настроек входов (см. п. 2.2.10) и настроек точек доступа (см. п. 2.2.9).

Удаление и добавление дочерних устройств, смена их адреса, а также редактирование свойств выходов и считывателей для контроллеров ЛКД-КС-2000 недоступны.

2.2.8.7 Настройка охранных контроллеров Elsys-AC2

Первоначальная настройка выполняется согласно п. 2.2.8.1, 2.2.8.2.

На вкладке дополнительных настроек (см. Рисунок 41) пользователю доступны опции «Параметры ввода PIN-кода» и «Использовать кольцевую топологию».

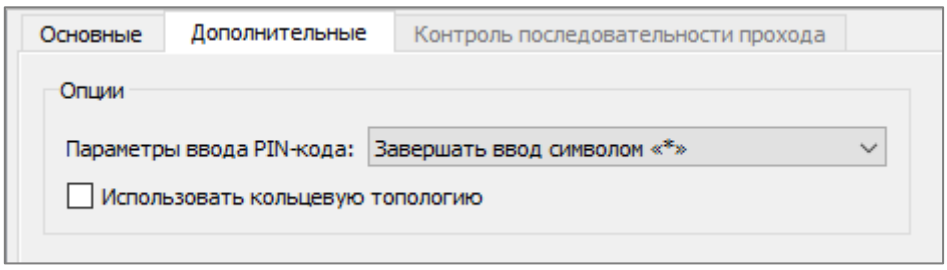

Рисунок 41. Дополнительны настройки контроллера Elsys-AC2

Описание настройки «Параметры ввода PIN-кода» дано в п. 2.2.8.4

При включенной опции «Использовать кольцевую топологию» контроллер отслеживает целостность кольцевой линии связи АДЛС и формирует при обрыве кольца событие «Нарушение кольцевой топологии», а при восстановлении целостности линии – событие «Восстановление кольцевой топологии».

2.2.8.8 Настройка клавиатур Elsys-CP2

Первоначальная настройка выполняется согласно п. 2.2.8.1, 2.2.8.2.

На вкладке дополнительных настроек (см. Рисунок 42) размещены следующие параметры клавиатуры: «Режим работы», «Отображение номеров индикаторов», «Идентификация пользователя», «Ориентация дисплея».

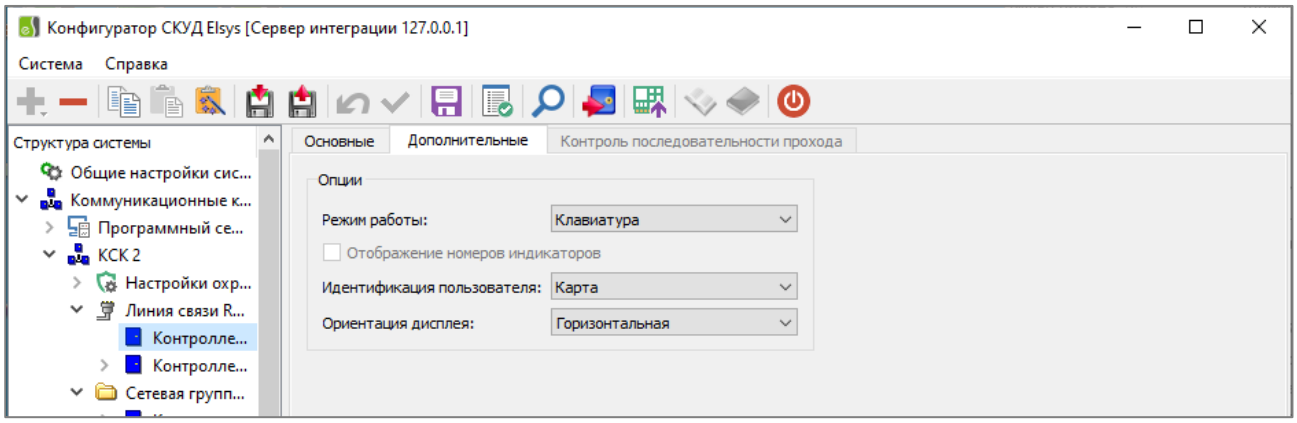

Рисунок 42. Дополнительные настройки клавиатуры Elsys-CP2

В клавиатуре предусмотрены два режима работы: «Клавиатура» и «Индикация и управление».

Режим «Клавиатура» обеспечивает управление охранными разделами в рамках полномочий пользователя, выполнившего авторизацию.

Режим «Индикация и управление» предусматривает непрерывный вывод на экран заранее назначенного набора разделов.

При использовании режима «Индикация и управление» доступна дополнительная настройка «Отображение номеров индикаторов». Если она включена, подписи на кнопках-индикаторах разделов на экране клавиатуры будут иметь числовые обозначения в диапазоне 1 – 40, а если выключена – в качестве подписей будут выводиться номера разделов.

Для клавиатуры предусмотрены способы идентификации:

– «Карта»;

– «PIN-код»;
– «Карта и PIN-код»;
– «Карта или PIN-код».

При выборе режима «Карта или PIN-код» пользователь может быть идентифицирован по любому признаку. При использовании способа идентификации «Карта и PIN-код» необходимо вводить оба признака (в любом порядке). В остальных способах идентификации используется только один указанный признак.

В поле «Ориентация дисплея» могут быть выбраны значения «Горизонтальная» или «Вертикальная», в зависимости от требуемого расположения клавиатуры.

Кроме настроек параметров клавиатуры, описанных в настоящей главе, необходимо выполнить настройку централизованной охранной подсистемы в КСК, под управлением которого работает клавиатура (см. документ «ТСОС Elsys. Руководство по эксплуатации»).

2.2.8.9 Настройка контроллера доступа Elsys-MB-SM

Первоначальная настройка выполняется согласно п. 2.2.8.1, 2.2.8.2.

В контроллерах доступа Elsys-MB-SM возможно добавление и настройка точек доступа типа «Дверь» и считывателей.

Входы и выходы контроллеров Elsys-MB-SM имеют фиксированное назначение, поэтому в конфигурации они отсутствуют.

2.2.9 Настройка точек доступа

В конфигураторе СКУД поддерживаются три типа точек доступа:

– дверь;
– ворота;
– турникет.

В состав оборудования точек доступа входят считыватели, датчики прохода и исполнительные устройства (замки, турникеты, приводы управления шлагбаумами и воротами).

2.2.9.1 *Добавление точек доступа*

Добавление точек доступа осуществляется из контекстного меню контроллера доступа (см. Рисунок 43) или кнопкой ✚ на панели быстрого доступа.

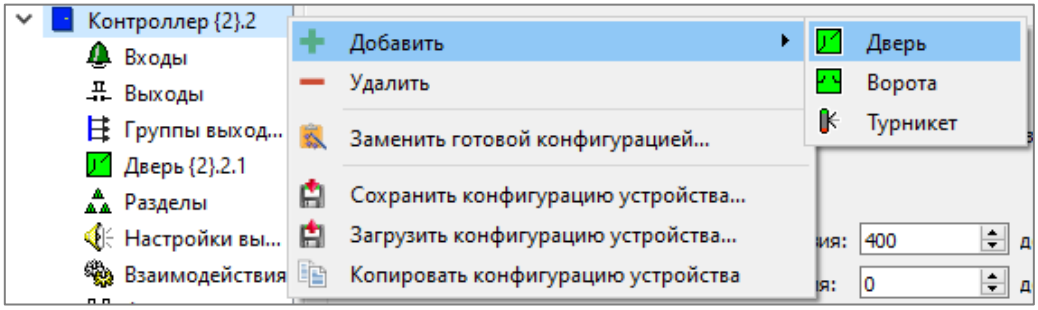

Рисунок 43. Добавление точек доступа из контекстного меню

В процессе настройки точек доступа потребуется добавить и настроить считыватели (см. п. 2.2.12), обслуживающие точку доступа, а также входы (см. п. 2.2.10) и выходы (см. п. 2.2.11), используемые в параметрах считывателей и точек доступа.

2.2.9.2 *Настройка двери*

Окно настройки параметров двери изображено на рисунке (Рисунок 44).

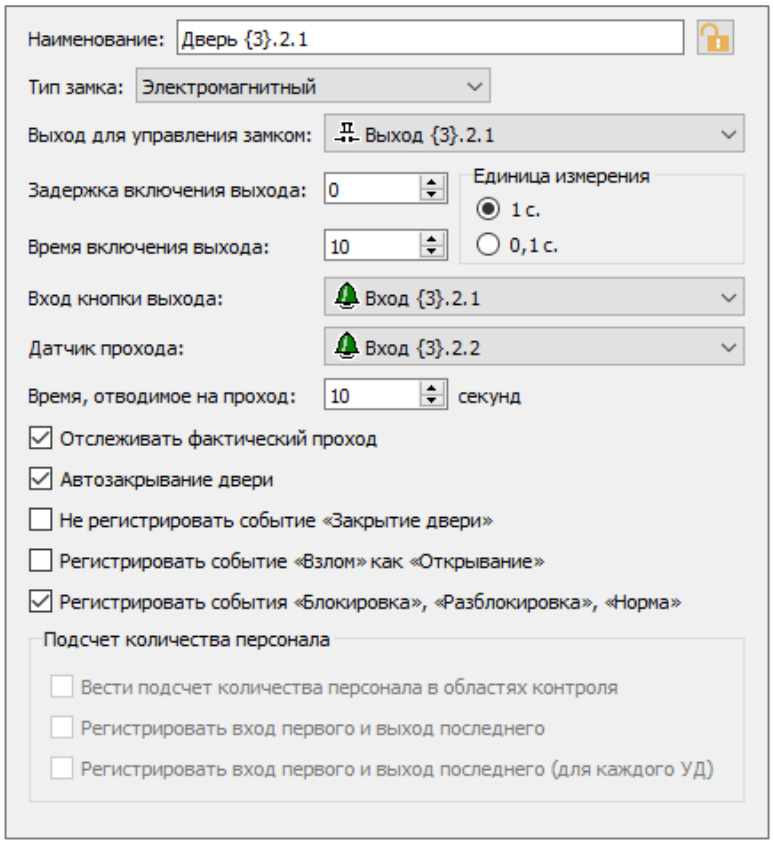

Рисунок 44. Окно настройки двери

При настройке двери с односторонним контролем доступа необходимо предварительно добавить в конфигурацию контроллера устройства, участвующие в её работе:

- выход для управления замком;
- входной считыватель;
- вход для подключения кнопки выхода;
- вход для подключения датчика прохода.

При настройке двери с двусторонним контролем доступа в конфигурацию контроллера необходимо добавить:

- выход для управления замком;
- входной считыватель;
- выходной считыватель;
- вход для подключения датчика прохода.

В качестве выхода для управления замком, как правило, используется релейный выход.

Для входа, предназначенного для подключения кнопки выхода, рекомендуется установить время интегрирования 70 мс, тип – в соответствии со схемой подключения (обычно – нормально разомкнутый).

Вход для подключения датчика прохода следует настроить в соответствии со схемой подключения датчика прохода (как правило, нормально замкнутый, время интегрирования 300 мс). Остальные опции входа роли не играют, их настраивать не нужно.

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

Ниже описано назначение настроек двери.

«Тип замка» – настройка, определяющая тип устройства, обеспечивающего приведение точки доступа в открытое или закрытое состояние. Настройка может принимать одно из значений: «Электромеханический» или «Электромагнитный». Электромеханические замки открываются кратковременной подачей напряжения, а электромагнитные – наоборот, снятием напряжения с замка на время, отведённое для прохода.

Тип замка «Электромеханический» следует выбирать, если в качестве исполнительного устройства используется электромеханический замок-защёлка, при использовании которого дверь после отпирания возвращается в закрытое состояние только после совершения прохода (открывания и закрывания двери). Во всех остальных случаях следует выбирать тип замка «Электромагнитный».

Для электромеханического замка предусмотрены следующие отличия в алгоритме работы:

– если замок был открыт, а проход не состоялся, контроллер по истечении времени, отводимого на проход, сформирует сообщение «Дверь не заперта»;
– если в точке доступа включен режим разблокировки, то при каждом закрытии двери контроллер будет формировать отпирающий импульс, возвращающий дверь в открытое состояние.

«Выход для управления замком» – выход контроллера, используемый для управления исполнительным устройством.

«Задержка включения выхода» (по умолчанию 0 с) – длительность задержки включения управляющего выхода в секундах (0 – 98 секунд с шагом 1 с, либо 0 – 9,8 секунд с шагом 0,1 с, в зависимости от выбранной единицы измерения).

«Время включения выхода» (по умолчанию 10 с) – время включения управляющего выхода в секундах (0 – 98 секунд с шагом 1 с, либо 0 – 9,8 секунд с шагом 0,1 с, в зависимости от выбранной единицы измерения). Для электромеханического замка устанавливается обычно минимальным (0,1 - 1 с), кроме того, рекомендуется использовать RC-цепочку, встроенную в источник питания контроллера (см. эксплуатационную документацию на оборудование). Для электромагнитного замка параметр «Время включения выхода» обычно устанавливается в диапазоне 5 – 30 секунд.

«Вход кнопки выхода» – вход контроллера, к которому подключается кнопка запроса на выход. Настройка используется только для дверей с односторонним контролем доступа.

«Датчик прохода» – вход контроллера, к которому подключается датчик прохода (как правило, это – нормально замкнутый магнитоконтактный датчик). Датчик прохода необходим для отслеживания состояния двери, регистрации

факта совершения прохода, а также для охраны помещения от несанкционированного доступа.

«Время, отводимое на проход» – время в секундах (0 – 98 с), в течение которого датчик прохода снимается с охраны для предоставления доступа. Обычно устанавливается в диапазоне 5 – 30 секунд. Если замок электромагнитный, то настройка должна иметь значение, равное или чуть большее, чем настройка «Время включения выхода». Если дверь была открыта и продолжает удерживаться в открытом состоянии, по окончании времени, отводимого на проход, сформируется тревожное событие «Удержание двери».

«Отслеживать фактический проход» – настройка, при включении которой проход регистрируется в момент открывания двери, а при выключении – одновременно с предоставлением доступа.

«Автозакрывание» – настройка, обеспечивающая в момент закрывания двери автоматическое выключение выхода, управляющего исполнительным устройством.

Опции «Не регистрировать событие «Закрытие двери», «Регистрировать событие «Взлом» как «Открывание»», «Регистрировать события «Блокировка», «Разблокировка», «Норма» включают или выключают регистрацию указанных событий.

2.2.9.3 Настройка ворот и шлагбаумов

Настройка заключается в конфигурировании в окне настроек ворот (см. Рисунок 45) следующих параметров:

«Датчик закрытого состояния» – вход контроллера, используемый для подключения датчика (как правило, нормально замкнутого), переходящего в нормальное состояние при полном закрытии ворот или шлагбаума. Также датчик используется для формирования события «Взлом» и регистрации фактического прохода.

«Датчик открытого состояния» – вход контроллера, используемый для подключения датчика (как правило, нормально разомкнутого), переходящего в нарушенное (замкнутое) состояние при полном открытии ворот или шлагбаума.

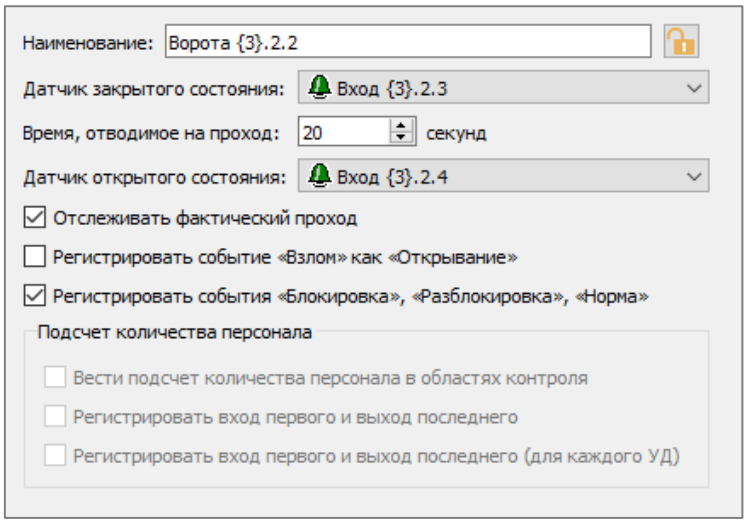

Рисунок 45. Окно настройки ворот

Назначение параметров «Время, отводимое на проход», «Регистрировать событие «Взлом» как «Открывание», «Регистрировать события «Блокировка», «Разблокировка», «Норма» аналогично назначению соответствующих параметров двери (см. п. 2.2.9.2).

2.2.9.4 Турникет

Окно настройки параметров турникета приведено на рисунке (Рисунок 46), в котором могут быть заданы параметры для обоих направлений прохода (обозначены как «входная точка», «выходная точка»).

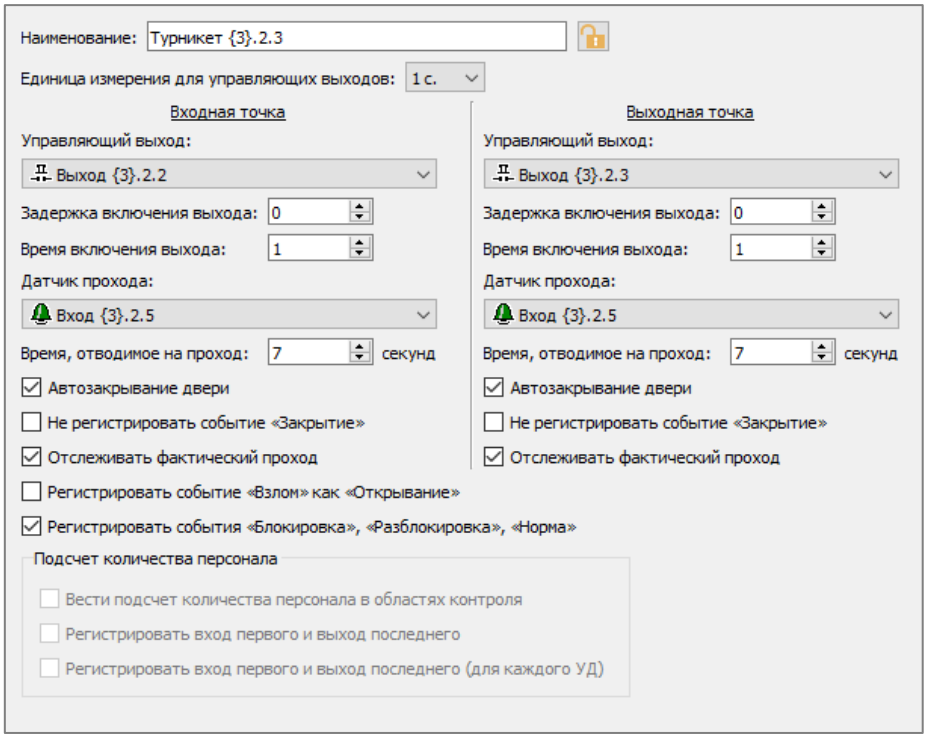

Рисунок 46. Окно настройки турникета

Назначение параметров аналогично назначению соответствующих параметров двери (см. п. 2.2.9.2).

2.2.10 Настройка входов

Добавление входов в конфигурацию контроллера осуществляется нажатием кнопки ✚ на панели быстрого доступа при выбранном узле «Входы» дерева устройств, либо из контекстного меню узла «Входы».

Окно конфигурации входа имеет вид, приведенный на рисунке (Рисунок 47).

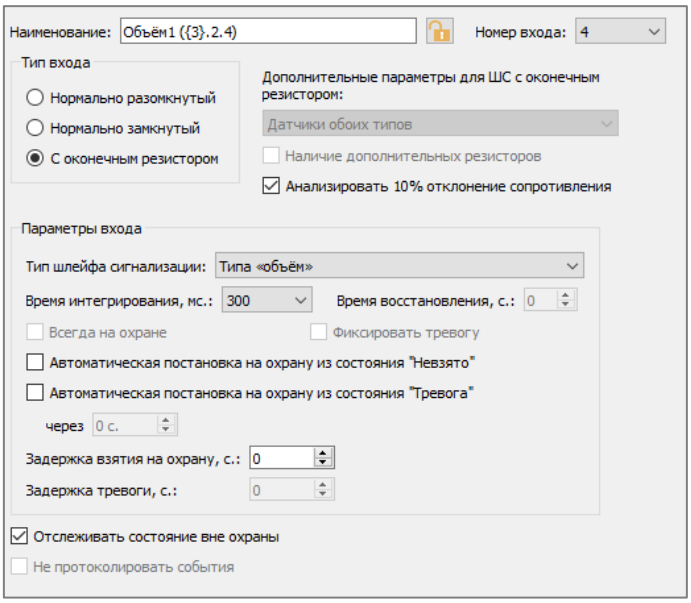

Рисунок 47.Окно настройки входа

«Наименование» – текстовое поле, которое формируется автоматически и может быть изменено пользователем.

«Номер входа» – порядковый номер (адрес), соответствующий расположению соответствующих клеммных соединителей на плате контроллера, либо адрес устройства в адресной двухпроводной линии (для охранного контроллера Elsys-AC2). Информация о количестве, типах и диапазоне возможных адресов входов для контроллеров разных типов приведена в эксплуатационной документации на оборудование.

Группа настроек «Тип входа» отвечает за то, какое состояние у входа будет считаться нормальным, при этом у аналоговых входов присутствует опция использования оконечного резистора и мониторинга отклонения его

сопротивления, что обеспечивает антисаботажную защиту при использовании входа для подключении шлейфа охранной сигнализации.

Опция «Тип шлейфа сигнализации» задаёт логику работы входа. Для этой настройки возможны значения:

- «Вход общего назначения»;
- «Охранный»;
- «Входной»;
- «Объём»;
- «Круглосуточный».

Если вход не предполагается использовать в охранной подсистеме, для него следует задавать тип «Вход общего назначения».

Тип «Охранный» задаётся для обычных охранных входов. При нарушении взятый на охрану вход немедленно переходит в состояние «Тревога». Состояние «Тревога» сохраняется до тех пор, пока вход не будет снят с охраны или повторно взят на охрану.

Тип «Входной» задаётся для входов, к которым подключены датчики проникновения, устанавливаемые на входе в помещение.

Тип «Объём» задаётся для входа, в который включены объёмные извещатели и иные датчики присутствия человека.

Тип «Круглосуточный» задаётся для входа, который всегда должен находиться на охране.

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

Устанавливать время интегрирования рекомендуется с учетом следующих критериев:

- 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).

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

«Всегда на охране» – опция означает, что вход всегда находится на охране. Эту опцию следует включать, если необходимо ограничить число состояний входа двумя – «Тревога» и «На охране». Это наиболее часто используемый режим работы входов общего назначения.

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

В таблице (Таблица 6) описана логика работы входа с типом ШС «Вход общего назначения» в зависимости от установленных опций «Всегда на охране» и «Фиксировать тревогу».

Таблица 13.

Логика работы входа с типом ШС «Вход общего назначения» в зависимости от значения опций «Всегда на охране» и «Фиксировать тревогу»

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

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

которых выключена настройка «Фиксировать тревогу», а также для входов, назначенных в качестве датчиков прохода точек доступа.

«Отслеживать состояние вне охраны» – при включенной опции состояние входа отслеживается, даже если вход не взят под охрану.

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

Если вход используется в конфигурации двери, турникета или считывателя, играет роль лишь группа настроек «Тип входа», параметры «Время интегрирования» и «Время восстановления» (для датчиков прохода), а параметр «Тип шлейфа сигнализации» должен иметь значение «Вход общего назначения».

Настройки «Автоматическая постановка на охрану из состояния «Невзято», «Автоматическая постановка на охрану из состояния «Тревога», «Задержка взятия на охрану», «Задержка тревоги» для входов общего назначения недоступны.

Подробное описание режимов работы и настройки охранных входов приведено в документе «ТСОС Elsys. Руководство по эксплуатации».

2.2.11 Настройка выходов и групп выходов

2.2.11.1 Настройка выходов

Добавление группы выходов осуществляется через панель быстрого доступа (см. Рисунок 6) или из контекстного меню в дереве устройств (см. Рисунок 48).

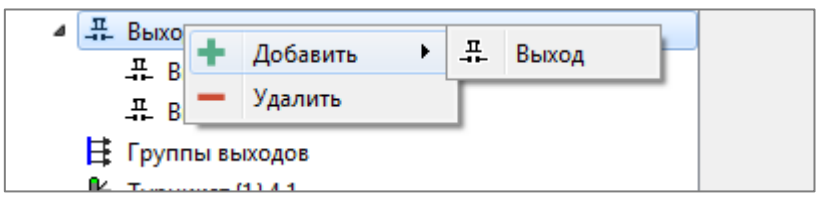

Рисунок 48. Добавление выходов из контекстного меню

Окно настройки выхода приведено на рисунке (Рисунок 49). Назначение настроек выхода описано ниже.

«Наименование» – текстовое поле, которое формируется автоматически и может быть изменено пользователем.

«Номер выхода» – номер выхода на плате контроллера либо адрес устройства в адресной двухпроводной линии (для охранного контроллера Elsys-AC2). Информация о количестве, типах и диапазоне возможных адресов выходов для контроллеров разных типов приведена в эксплуатационной документации на оборудование.

Рисунок 49. Окно формы настройки выхода

При включении опции «Инвертировать выход» выход переходит в нормально замкнутый режим работы, при отключении – в нормально разомкнутый.

При включении опции «Мониторинг состояния выхода» контроллер регистрирует в протоколе событий изменения состояния выхода.

При включении опции «Мониторинг окончания работы выхода» контроллер регистрирует в протоколе сообщение об окончании работы по формуле.

2.2.11.2 Настройка групп выходов

Группы выходов поддерживаются в контроллерах доступа Elsys-MB (кроме Elsys-MB-SM) и Elsys-NG-xx.

Добавление группы выходов осуществляется через панель быстрого доступа (см. Рисунок 6) или из контекстного меню в дереве устройств (см. Рисунок 50).

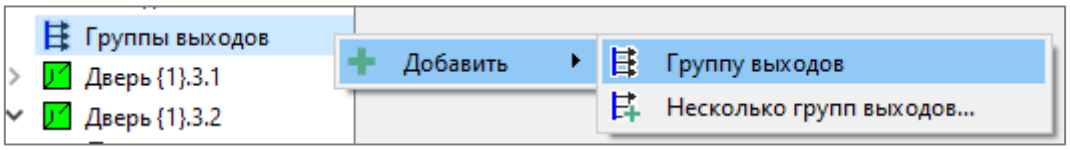

Рисунок 50. Добавление группы выходов из контекстного меню

Настройка основных свойств групп выходов аналогична настройке выходов (см. Рисунок 49), за исключением того, что группа не может быть инверсной.

Группа выходов является логическим объединением нескольких выходов для одновременного обращения к ним как к обычному выходу.

Группа выходов может быть пустой. Для каждого контроллера может быть создано до 12 групп выходов. Любые выходы могут входить в состав любых групп, в том числе нескольких. Добавление в группу осуществляется выбором выходов в списке «Доступные выходы» и последующим нажатием кнопки для переноса их в список «Выходы в группе». Аналогичным образом выходы убираются из группы с использованием кнопки. Также перенос из одного списка в другой можно осуществить двойным щелчком левой кнопки мыши на выход, который требуется добавить или исключить из группы.

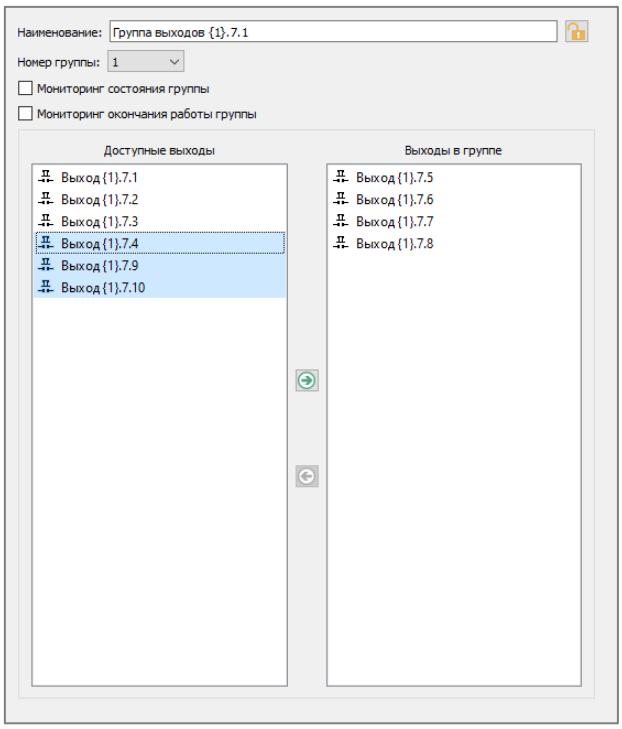

Рисунок 51. Окно настройки группы выходов

2.2.12 Настройка считывателей

Каждый контроллер имеет возможность работать только с одним типом подключения считывателей. Совместная работа считывателей с разными интерфейсами невозможна. Выбор интерфейса считывателей выполняется в окне основных настроек контроллера.

Считыватель можно добавить в конфигурацию контроллеров доступа и охранных контроллеров. Для добавления используется кнопка «Добавить новый элемент дерева устройств», так же можно использовать добавление из контекстного меню контроллера (для охранных контроллеров см. Рисунок 52) или точки доступа (для контроллеров доступа см. Рисунок 53).

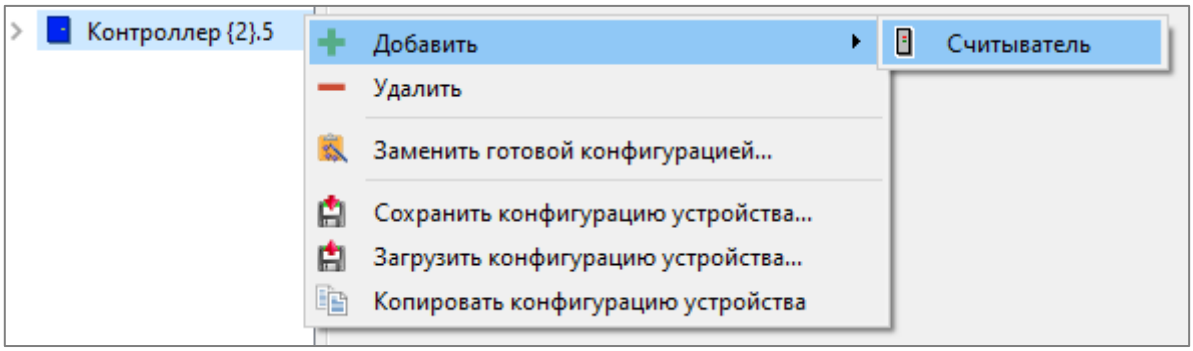

Рисунок 52.Добавление считывателя в конфигурацию охранного контроллера

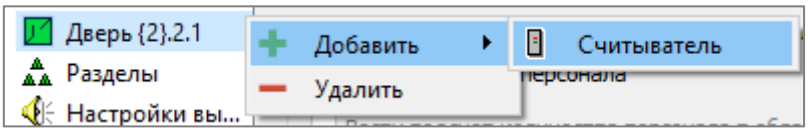

Рисунок 53.Добавление считывателя в конфигурацию контроллера доступа

2.2.12.1 Основные настройки считывателя

Основные настройки считывателя (см. Рисунок 54) описаны ниже.

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

«Наименование» – текстовый идентификатор считывателя. По умолчанию содержит в составе текста часть, обозначающую точку доступа, к которой относится этот считыватель. Имя считывателя используется при настройке уровней доступа в программном обеспечении бюро пропусков.

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

«Использовать устройства» – возможны три варианта использования устройств идентификации: только считыватель, считыватель и клавиатура, только клавиатура.

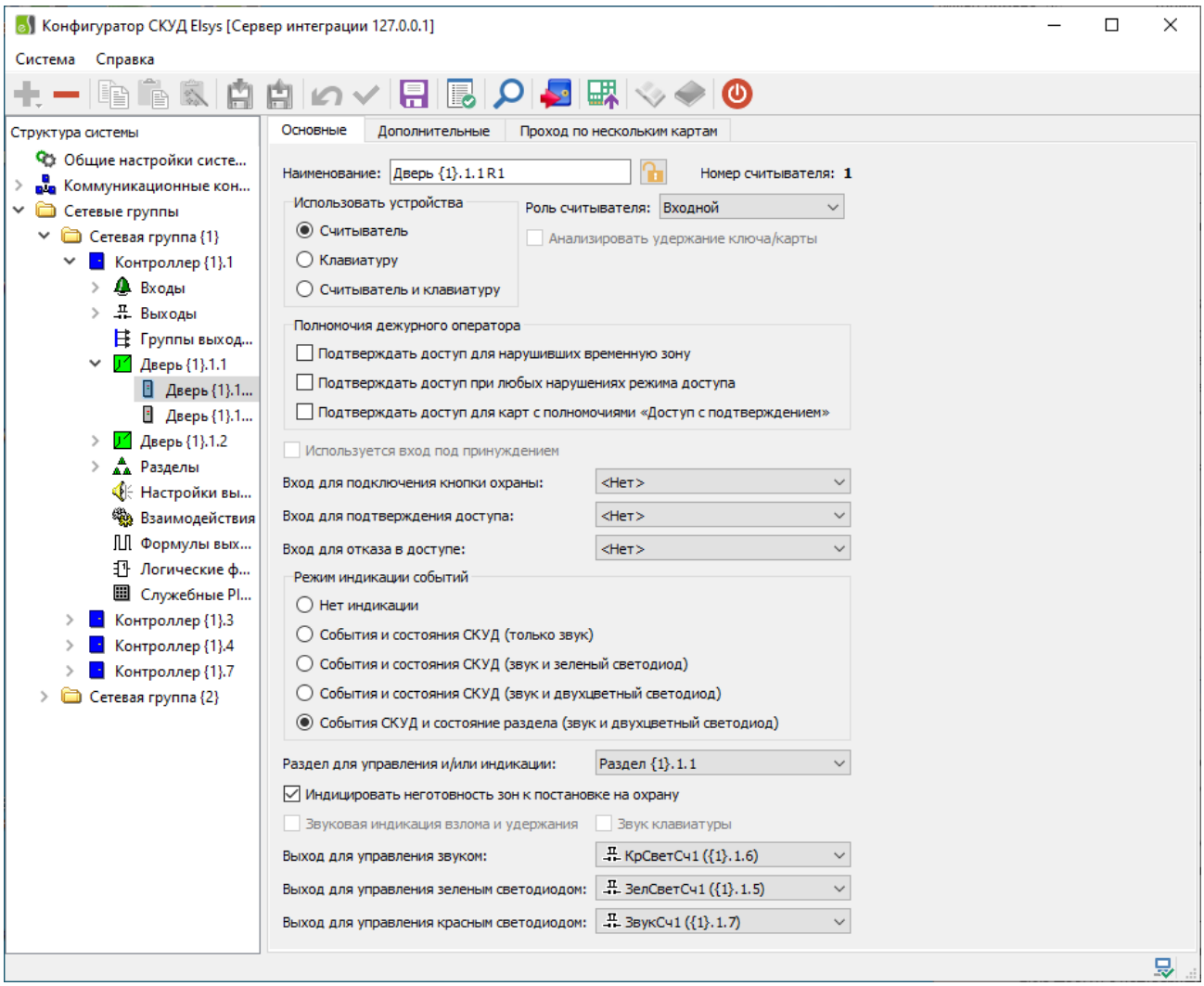

Рисунок 54. Основные настройки считывателя

Группа настроек «Полномочия дежурного оператора», к которым относятся настройки «Подтверждать доступ для нарушивших временную зону», «Подтверждать доступ при любых нарушениях режима доступа», «Подтверждать доступ для пользователей с полномочиями «Доступ с подтверждением» задаёт категории пользователей системы, доступ которым может быть предоставлен дежурным оператором нажатием кнопки «Подтверждение доступа» (при этом регистрируется соответствующее событие).

«Используется вход под принуждением» – если эта опция включена, то при наличии клавиатуры становится возможным использовать режим «Доступ под принуждением». Если используется этот режим, пользователь системы может набрать «принудительный» PIN-код, предъявить карту и получить право доступа, точно так же, как и при штатном предъявлении карты, но при этом

сформируются события «Предоставление доступа под принуждением», затем «Вход/выход под принуждением», являющиеся тревожными сообщениями для дежурного оператора.

«Принудительный» PIN-код отличается от штатного младшей цифрой, которая вычисляется следующим образом: если младшая цифра PIN-кода в диапазоне 0 – 4, необходимо прибавить число 5, если младшая цифра в диапазоне 5 – 9, необходимо отнять число 5. При использовании доступа под принуждением необходимо проследить, чтобы ни один «принудительный» код не совпадал со штатным PIN-кодом. Например, диапазонам штатных PIN-кодов: 1 – 4, 15 – 24 и 35 – 44 соответствуют диапазоны «принудительных» PIN-кодов: 6 – 14, 25 – 34 и 45 – 49.

«Вход для подключения кнопки охраны» – вход для подключения кнопки, используемой для управления режимами охраны. При нажатой кнопке одно- и двукратное предъявление карты соответствующему считывателю интерпретируется как события «Постановка на охрану» и «Снятие с охраны» соответственно. Для использования этих событий необходимо настроить взаимодействия.

«Вход для подтверждения доступа» и «Вход для отказа в доступе» – входы контроллера, используемые для подключения кнопок подтверждения или отказа в доступе. Если точка доступа двусторонняя, то для входного и выходного считывателя эти настройки могут совпадать.

«Режим индикации событий» – настройка, определяющая режим индикации считывателя и набор необходимых линий индикации. Возможные значения настройки:

- «Индикация отсутствует»;
- «События и состояния СКУД (только звук)»;
- «События и состояния СКУД (звук и зелёный светодиод)»;
- «События и состояния СКУД (звук и двухцветный светодиод)»;
- «События СКУД и состояние раздела (звук и двухцветный светодиод)».

Рекомендуется использовать режим «События и состояния СКУД (звук и двухцветный светодиод)», а при использовании считывателя для управления режимами охраны – «События СКУД и состояние раздела (звук и двухцветный

светодиод)». Эти режимы описаны в таблицах (Таблица 9, Таблица 10) соответственно.

Режимы «События и состояния СКУД (только звук)» и «События и состояния СКУД (звук и зелёный светодиод)» оставлены для совместимости с предыдущими версиями контроллеров, их использовать не рекомендуется.

В выпадающих списках настроек «Выход управления звуком», «Выход управления зелёным светодиодом», «Выход управления красным светодиодом» назначаются выходы контроллера, заданные пользователем для подключения соответствующих входов считывателя, использующего интерфейс Wiegand или Touch Memory. При использовании интерфейсов ESDP и «ESDP защищённый» эти настройки недоступны, а входы и выходы контроллера, предназначенные для подключения считывателей, могут использоваться как входы и выходы общего назначения.

Настройка «Раздел для управления и/или индикации» назначает раздел, состояние которого будет индицироваться светодиодами и звуковым сигнализатором считывателя в режиме индикации «События СКУД и состояние раздела (звук и двухцветный светодиод)». Кроме того, назначенным разделом можно управлять, используя кнопку управления охраной или удерживая карту.

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

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

Настройка «Звуковая индикация взлома и удержания» (актуальна для режимов индикации «События и состояния СКУД (…)») обеспечивает звуковую индикацию состояний точки доступа «Взлом» и «Удержание».

«Звук клавиатуры» – если включена эта опция, то каждое нажатие на клавиатуре, относящейся к считывателю, подключенному по интерфейсу Wiegand, будет сопровождаться коротким звуковым сигналом на выходе для управления звуком этого считывателя.

Из описанных выше настроек для охранных контроллеров Elsys-AC2 и Elsys-MB-AC используются только настройки «Наименование» и «Использовать устройства», а для контроллеров Elsys-MB-SM — «Наименование», «Использовать устройства» и «Роль считывателя».

2.2.12.2 Дополнительные настройки считывателя

Дополнительные настройки считывателей размещены на вкладке «Дополнительные» (см. Рисунок 55).

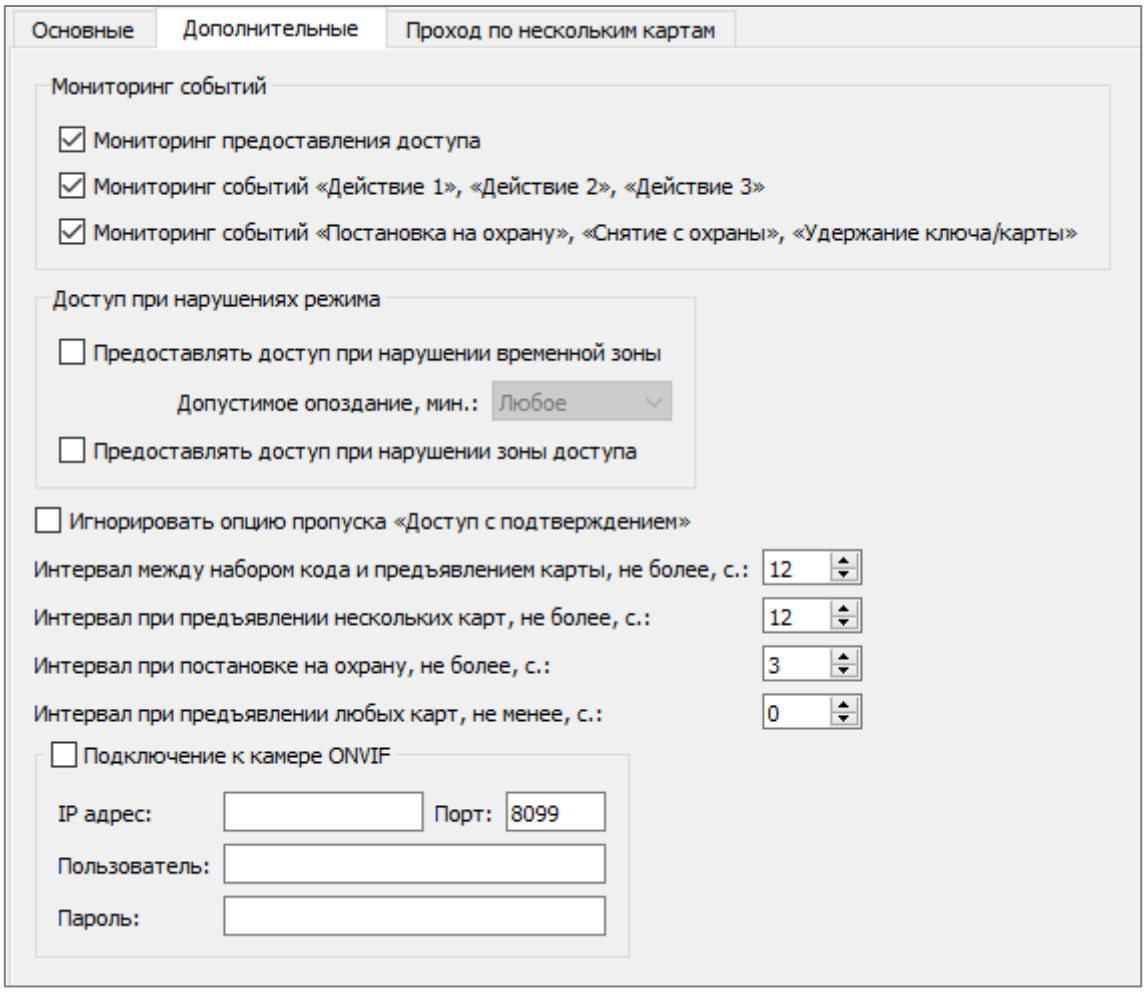

Рисунок 55. Дополнительные настройки считывателя

В группе настроек «Мониторинг событий» выбираются события, соответствующие наименованиям опций, которые будут регистрироваться контроллером.

Группа настроек «Доступ при нарушениях режима» позволяет задать настройки таким образом, чтобы после регистрации нарушения пользователю был предоставлен доступ.

Если включена опция «Предоставлять доступ при нарушении временной зоны», то при нарушении временной зоны сначала формируется событие «Нарушение временной зоны», а затем предоставляется доступ. В сочетании с этой настройкой может использоваться опция «Допустимое опоздание», которая позволяет задать время, по истечении которого предоставление доступа будет запрещено.

Если включена опция «Предоставлять доступ при нарушении зоны доступа», то в режиме глобального контроля последовательности прохода при нарушении зоны доступа после формирования события «Нарушение зоны доступа» предоставляется доступ.

Опция «Игнорировать опцию пропуска «Доступ с подтверждением» позволяет для отдельного считывателя не использовать дополнительный параметр пропуска «Доступ с подтверждением» (этот параметр распространяется на контроллер, а в действительности он необходима для отдельных считывателей; для считывателей, где он не нужен, следует включать настройку «Игнорировать опцию пропуска «Доступ с подтверждением»).

«Интервал между набором кода и предъявлением карты» (1 – 127 с) задаёт максимальное время, в течение которого считыватель будет ожидать предъявления карты до сброса введённого PIN-кода.

«Интервал при предъявлении нескольких карт» (1 – 127 с) – максимальное время, в течение которого можно предъявить следующую карту, если настроен проход по нескольким картам.

«Интервал при постановке на охрану» (0 – 127 с) – максимальное время, в течение которого должна быть повторно предъявлена карта для управления охраной. По истечении временного интервала, если карта не была предъявлена повторно, выполняется постановка на охрану, а если была предъявлена – выполняется снятие с охраны.

«Интервал при предъявлении любых карт» (0 – 127 с) – параметр, который задаёт минимальное время, в течение которого, после предъявления последней карты, считыватель не реагирует на предъявление следующих карт.

Описанные выше настройки недоступны для охранных контроллеров Elsys-AC2 и Elsys-MB-AC.

Для контроллеров Elsys-MB-SM доступны только настройки «Мониторинг предоставления доступа» и настройки из группы «Доступ при нарушениях режима».

2.2.12.3 Настройка прохода по нескольким картам

Параметры считывателей, используемые при настройке доступа по правилу двух (трёх) лиц, находятся на вкладке «Проход по нескольким картам» (см. Рисунок 56) и описаны ниже.

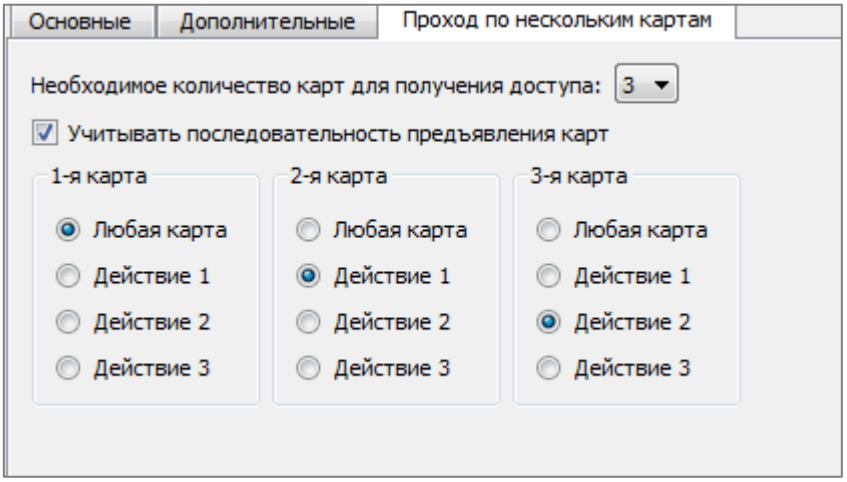

Рисунок 56. Вкладка настройки прохода по нескольким картам

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

Для каждой из последовательно предъявляемых карт могут быть заданы опции, необходимые для получения доступа (возможные варианты – «Любая карта», «Действие 1», «Действие 2», «Действие 3»). Опция «Любая карта» означает, что может быть предъявлена карта с любыми полномочиями, в то время как выбранная опция с наименованием «Действие …» требует указанных полномочий от предъявляемой карты.

Если включена настройка считывателя «Учитывать последовательность предъявления карт», карты следует предъявлять в строго определённом порядке, в зависимости от необходимых опций. Если эта настройка выключена, порядок предъявления карт роли не играет.

Опции для настройки прохода по нескольким картам актуальны для контроллеров доступа Elsys-MB (кроме Elsys-MB-SM) и Elsys-NG-xx.

2.2.12.4 Настройка подключения к ONVIF камере

Для контроллеров доступа Elsys-NG-800 и Elsys-NG-1000 поддерживается функция контроля и санкционирования доступа по государственному регистрационному знаку автомобиля (далее автомобильный номер) при совместной работе с видеокамерами, оснащёнными встроенной аналитикой распознавания автомобильных номеров и поддерживающими обмен информацией по протоколу, совместимому со спецификацией ONVIF.

При выборе модели видеокамеры необходимо уточнить параметры совместимости видеокамеры и протокола передачи данных, обратившись в службу технической поддержки ГК «ТвинПро» для согласования перечня поддерживаемых видеокамер.

Подключение камеры осуществляется в одну сеть с контроллером, для привязки камеры к считывателю требуется корректно заполнить поля «IP адрес», «Порт», «Пользователь» и «Пароль». Подробная информация о настройке камер приведена в документации на используемую камеру.

Считывание распознанного автомобильного номера полностью эквивалентно предъявлению карты доступа. Все настройки считывателей и взаимодействий с их использованием будут работать при анализе распознанных номеров, при этом считыватель будет формировать события только от номеров, содержащейся во внутренней базе данных контроллера.

2.2.12.5 Настройка считывателей с интерфейсом ESDP

Протокол ESDP обеспечивает контроль состояния связи со считывателем, контроль состояния корпуса, передачу кода вещественного идентификатора. Также доступны функции централизованной инициализации считывателей и обновления прошивок.

Перед подключением считывателя в линию ESDP контроллера следует убедиться, что контроллер и считыватель поддерживают этот протокол. Информация о поддержке протокола отражена в руководствах по эксплуатации на используемые контроллер и считыватель.

Протокол ESDP поддерживается в контроллерах доступа Elsys-NG-800 (начиная с версии прошивки 4.14), Elsys-NG-1000 (начиная с версии прошивки 5.07), охранных контроллерах Elsys-AC2 (начиная с версии прошивки 1.10).

Перед настройкой считывателей с поддержкой протокола ESDP необходимо в окне основных настроек контроллера выбрать интерфейс «ESDP» или «ESDP защищённый» и задать необходимую скорость обмена (см. Рисунок 57).

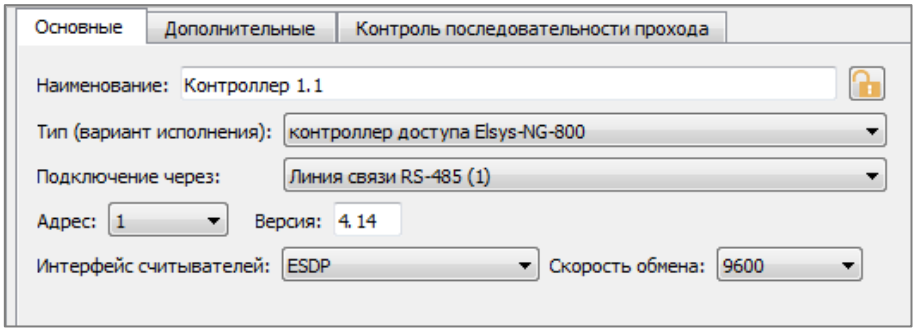

Рисунок 57. Выбор интерфейса ESDP в окне свойств контроллера

При использовании интерфейса ESDP после выполнения настроек в контроллере и его инициализации, необходимо настроить параметры ESDP в самих считывателях, чтобы контроллер установил с ними связь.

Считыватель, поддерживающий протокол ESDP, автоматически на него переключается после начала опроса контроллером, в котором установлен соответствующий интерфейс. В одной линии все периферийные устройства должны иметь уникальный адрес и одинаковую скорость обмена, на которую настроен контроллер. Адрес должен соответствовать номеру считывателя в конфигурации. Смена адреса и скорости обмена в считывателе может быть выполнена либо в окне поиска (см. п. 2.2.2.6), либо иным способом (см. руководство по эксплуатации на конкретный считыватель).

Проверить состояние связи со считывателем можно в окне инициализации, при условии, что сам контроллер на связи и проинициализирован. Если контроллер установил соединение со считывателями, то они будут отображаться как активные элементы (см. Рисунок 58).

В настройках считывателя, если выбран интерфейс ESDP или «Защищённый ESDP» становятся доступны настройки «Тип» и «Версия»

(см. Рисунок 59), а также вкладки с конфигурацией считывателя: «Параметры ESDP (основные)», «Параметры ESDP (дополнительные)». Настройки на дополнительных вкладках загружаются непосредственно в сами считыватели при инициализации.

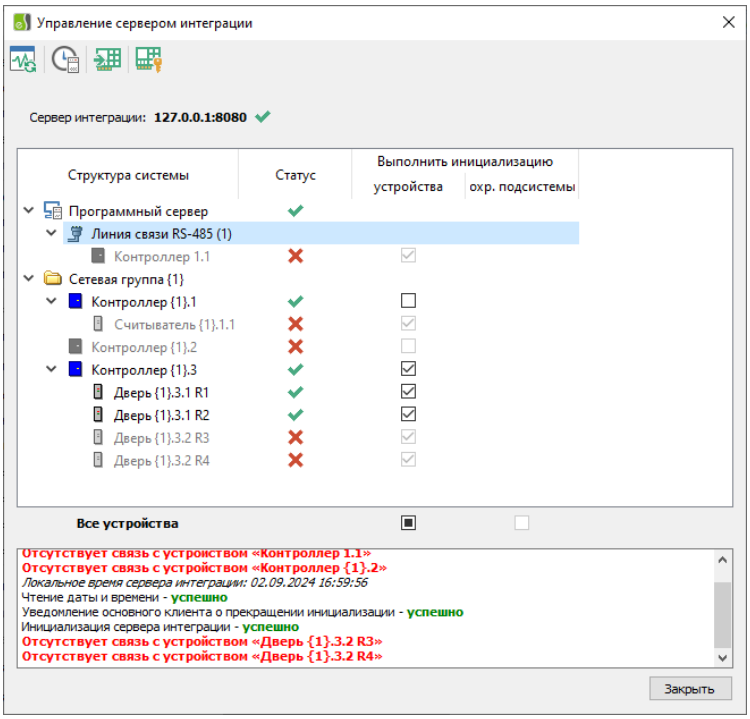

Рисунок 58. Окно инициализации с отображением считывателей

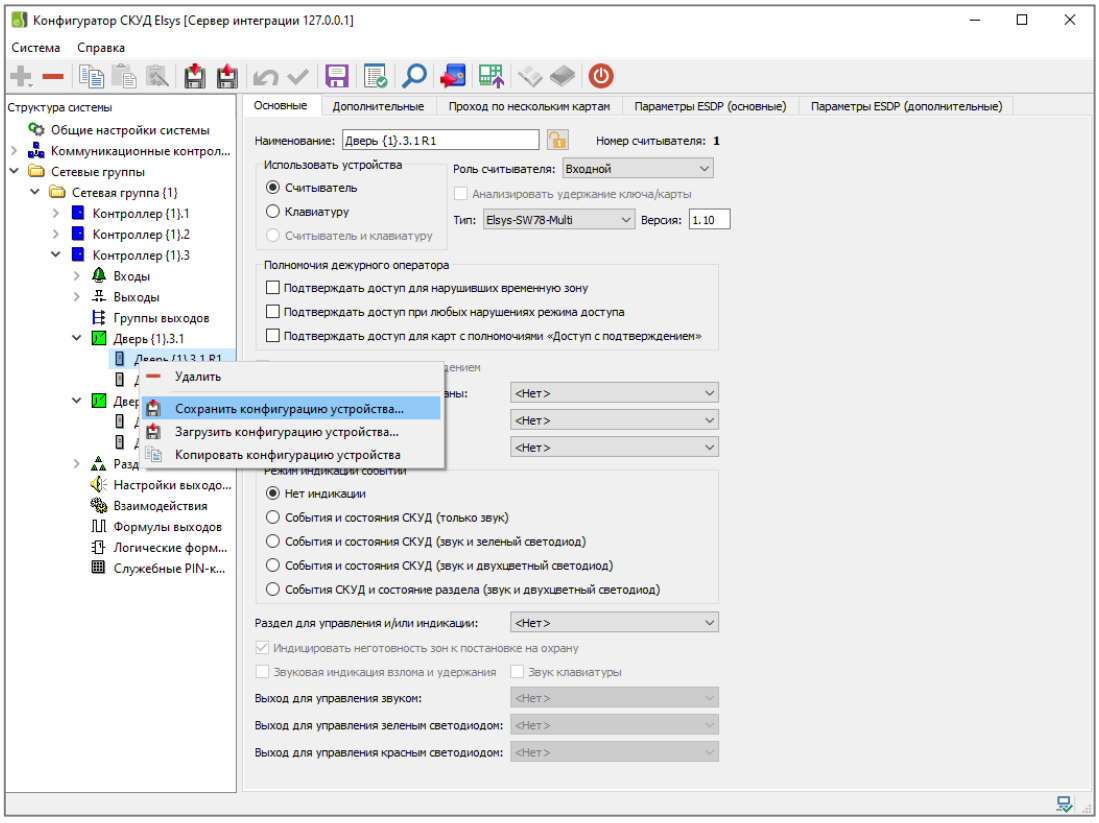

Рисунок 59. Окно основных настроек считывателя ESDP

Конфигурацию считывателя можно сохранить в файл либо загрузить из файла из контекстного меню считывателя или с помощью кнопок на панели быстрого доступа (см. Рисунок 59). Также предусмотрена возможность копирования конфигураций ESDP-считывателей.

В полях «Тип» и «Версия» должна быть указана актуальная информация. Для её обновления можно воспользоваться окном поиска ESDP устройств (см. п. 2.2.2.6). Для разных типов считывателей могут быть доступны разные настройки. Поле «Тип» также используется для проверок при обновлении прошивки.

Все настройки считывателей, описанные в пунктах 2.2.12.1, 2.2.12.2 и 2.2.12.3, за исключением настроек «Выход для управления звуком», «Выход для управления зелёным светодиодом», «Выход для управления красным светодиодом», актуальны и при использовании интерфейса ESDP.

Входы и выходы, предназначенные для подключения считывателей с интерфейсами Wiegand или Touch Memory, при использовании интерфейса ESDP могут использоваться в качестве входов и выходов общего назначения.

Основные настройки считывателей с интерфейсом ESDP размещены на вкладке «Параметры ESDP (основные)» (см. Рисунок 60) и описаны ниже.

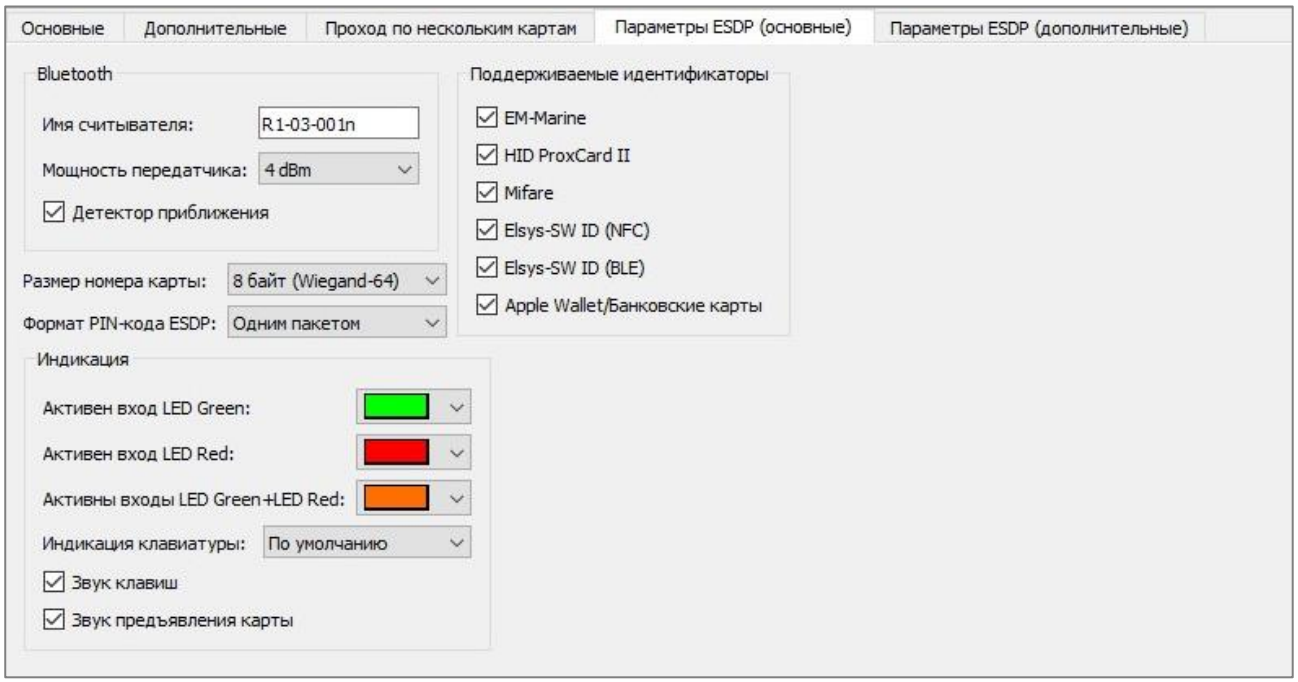

Рисунок 60. Параметры ESDP (основные)

«Имя считывателя» – отображается при поиске по интерфейсу BLE (Bluetooth low energy).

«Мощность передатчика» – мощность передатчика BLE.

«Детектор приближения» – настройка включает детектор приближения для определения поднесения телефона при идентификации по BLE.

«Размер номера карты» – настройка устанавливает ограничение на длину отправляемого кода по ESDP для совместной работы в системе со считывателями, подключенными по интерфейсу Wiegand.

«Активен вход LED Green» – настройка меняет зелёный цвет в индикациях событий.

«Активен вход LED Red» – настройка меняет красный цвет в индикациях событий.

«Активны входы LED Green + LED Red» – настройка меняет жёлтый цвет в индикациях событий.

«Индикация клавиатуры» (только для клавиатурных считывателей) – настройка устанавливает один из предустановленных режимов индикации клавиатуры считывателя.

«Звук клавиш» (только для клавиатурных считывателей) – если настройка включена, то нажатие клавиш считывателя будет сопровождаться коротким звуковым сигналом.

«Звук предъявления карты» – если настройка включена, то предъявление идентификатора считыватель будет сопровождать коротким звуковым сигналом.

«Поддерживаемые идентификаторы» – настройка включает или выключает чтение соответствующих типов идентификаторов.

Дополнительные настройки считывателей с интерфейсом ESDP размещены на вкладке «Параметры ESDP (дополнительные)» (см. Рисунок 61) и описаны ниже.

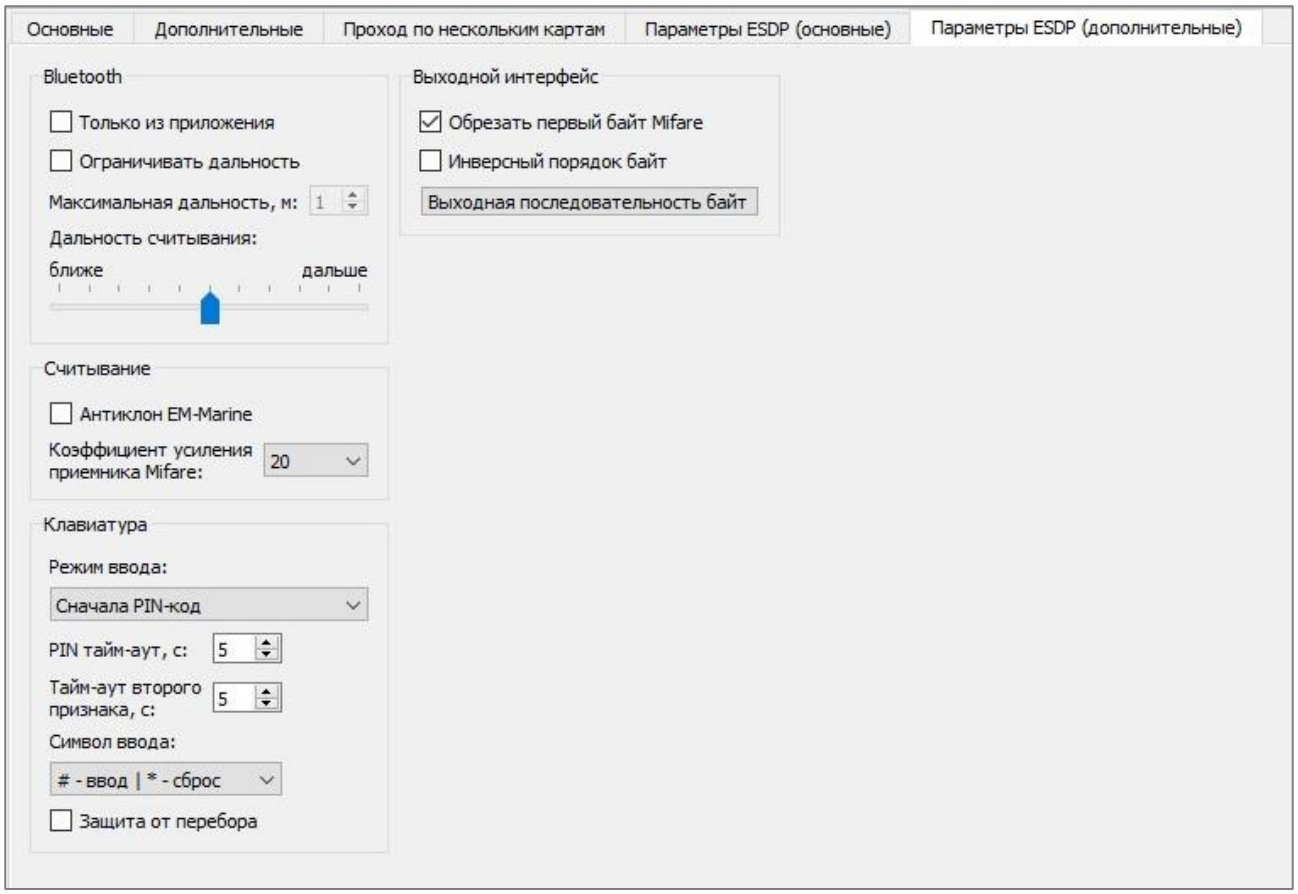

Рисунок 61. Параметры ESDP (дополнительные)

«Только из приложения» – настройка включает или выключает режим «Свободные руки» для идентификации по BLE.

«Ограничивать дальность» – настройка включает или отключает ограничение дальности подключения по BLE.

«Максимальная дальность» – если включена настройка «Ограничивать дальность», то устанавливает приблизительное значение ограничения дальности подключения по BLE.

«Дальность считывания» – настройка корректирует вычисление дальности пользовательского устройства при подключении по BLE.

«Антиклон EM-Marine» – настройка включает или выключает определение клона карты EM-Marine (функция не гарантирует 100 % вероятности определения клона).

«Коэффициент усиления приёмника Mifare» – настройка задаёт коэффициент усиления приёмника Mifare, который влияет на качество чтения некоторых карт.

«Режим ввода» (только для клавиатурных считывателей) – настройка устанавливает последовательность ввода идентификаторов.

«PIN тайм-аут» (только для клавиатурных считывателей) – устанавливает время в секундах, на которое считыватель будет включать полную яркость подсветки клавиатуры после начала ввода.

«Тайм-аут второго признака» (только для клавиатурных считывателей) – настройка устанавливает время в секундах, в течение которого считыватель будет ожидать ввод второго признака.

«Символ ввода» (только для клавиатурных считывателей) – настройка устанавливает назначение спец символов «#», «*» клавиатуры (должно соответствовать настройке в контроллере).

«Защита от перебора» (только для клавиатурных считывателей) – если эта настройка включена, то при вводе трёх PIN-кодов подряд в течение 10 секунд, считыватель перестанет реагировать на ввод в течение 30 секунд, что значительно усложняет его подбор. Важно учитывать, что считыватель не анализирует корректность PIN-кода, т.е. если были введены три штатных кода подряд, то ввод также заблокируется.

«Обрезать первый байт Mifare» – если эта настройка включена, то считыватель будет отбрасывать нулевой байт UID7 и UID10, в котором хранится код производителя карт Mifare.

«Инверсный порядок байт» – меняет порядок следования байт кода идентификатора.

«Выходная последовательность байт» (только для опытных пользователей) – настройка позволяет задать произвольное смещение в коде идентификатора и добавить неизменяемые байты.

После смены настроек считывателя его необходимо проинициализировать. В окне инициализации оборудования (см. Рисунок 58) устройства, в которых были изменения, автоматически выбираются для инициализации. При необходимости можно скорректировать автоматический выбор считывателей и затем запустить инициализацию оборудования.

Протокол ESDP частично совместим с протоколом OSDP и обеспечивает передачу состояния тампера и кода вещественного идентификатора. При этом поддержка устройств с OSDP сторонних производителей не гарантируется.

2.2.12.6 Настройка защищённого протокола ESDP

Режим «Защищённый ESDP» обеспечивает защиту канала связи между контроллером и считывателем, защиту от подмены считывателя, защиту от извлечения и подлога кода вещественного идентификатора. Также в этом режиме доступны централизованные функции.

Перед установкой защищённого соединения сначала необходимо убедиться, что контроллер устанавливает связь со считывателем по ESDP (см. Рисунок 58). Во время первоначальной настройки защищённого соединения должна обеспечиваться безопасность линии связи. Рекомендуется сначала подключать считыватели в непосредственной близости к контроллеру, а после настройки защищённого соединения устанавливать их на штатные места.

Для установки защищённого соединения необходимо выбрать в конфигурации контроллера интерфейс считывателя «Защищённый ESDP» и провести его инициализацию. После загрузки новой конфигурации начнётся процесс установки защищённого соединения, в результате которого контроллер и считыватель обменяются секретной информации, на основании которой они будут идентифицировать друг друга.

После установки защищённого соединения в считывателе становятся недоступны интерфейсы Wiegand, Touch Memory и ESDP. Также связь по защищённому ESDP может быть установлена только с сопряжённым контроллером. Для подключения считывателя по другому интерфейсу или к другому контроллеру, необходимо вернуть его настройки к заводским установкам, выполнив очистку конфигурации.

Это можно сделать собственными средствами устройства (см. руководство по эксплуатации на конкретное изделие), либо с помощью окна поиска ESDP устройств (см. п. 2.2.2.6). При этом будут очищены и все параметры безопасности.

Контроллер после установки защищённого соединения также будет подключаться только к сопряжённому считывателю. Для смены считывателя необходимо выполнить очистку конфигурации контроллера (см. руководство по эксплуатации на конкретное изделие), при этом подключение прежнего периферийного устройства без очистки его конфигурации будет невозможно.

Защищённый режим ESDP частично совместим с аналогичным протоколом OSDP. При этом подключение устройств сторонних производителей по защищённому OSDP не гарантируется, а процесс установки соединения может отличаться.

2.2.13 Настройка локальных охранных функций

Локальное управление охранной сигнализацией 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.

Настройка охранных функций заключается в конфигурировании разделов сигнализации и выходов оповещения, и, при необходимости – в настройке взаимодействий и некоторых параметров считывателей.

Окно настройки охранных разделов приведено на рисунке (Рисунок 62), а окно настройки выходов оповещения – на рисунке (Рисунок 63).

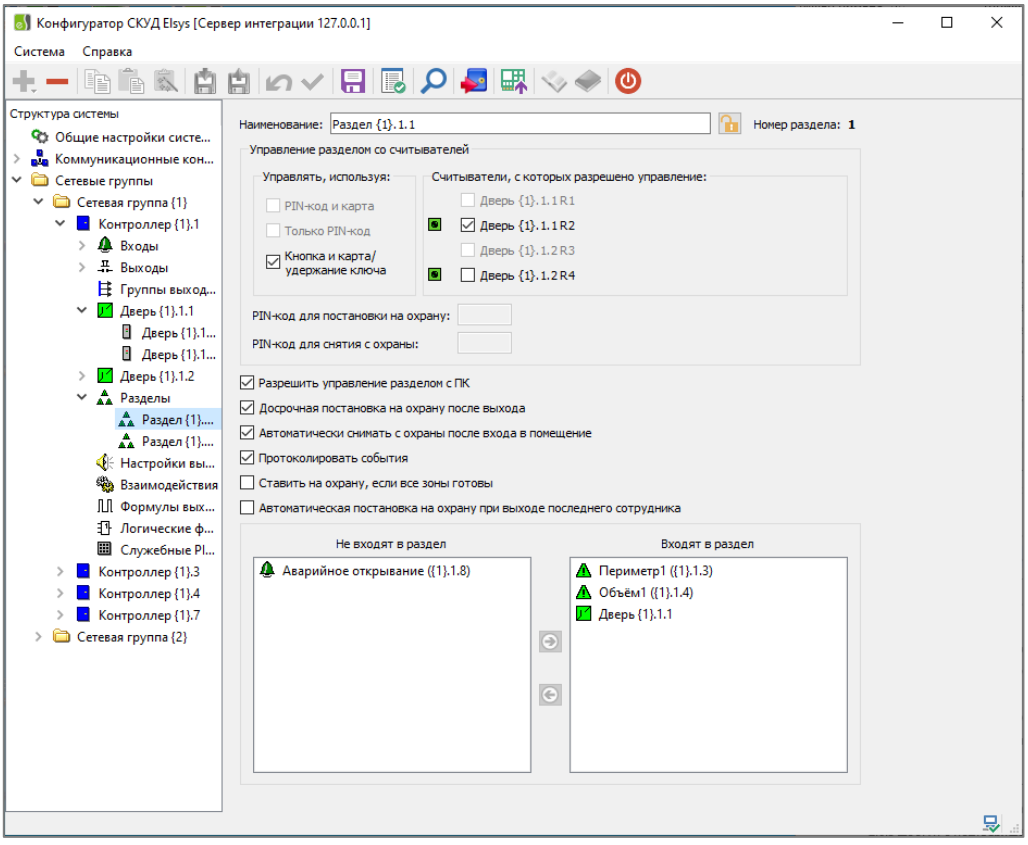

Рисунок 62. Окно настройки локального раздела

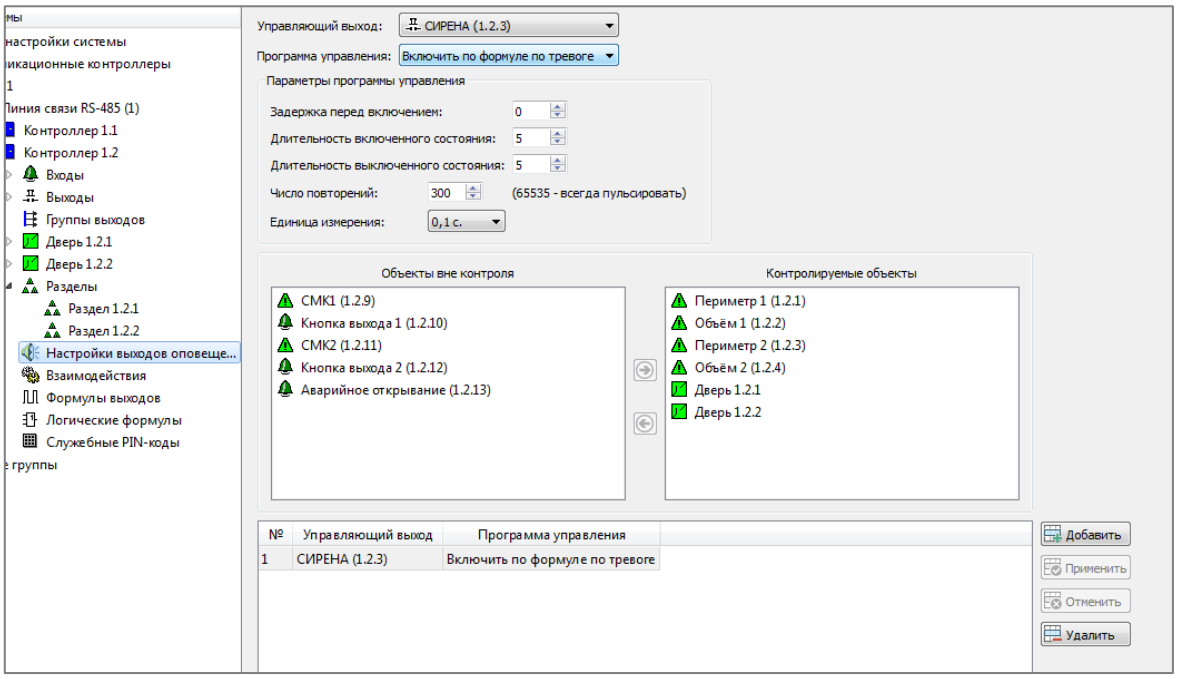

Рисунок 63. Окно настройки выходов оповещения

Настройка охранной подсистемы описана в документе «ТСОС Elsys. Руководство по эксплуатации».

2.3 Система программируемых аппаратных взаимодействий

2.3.1 Общие сведения

Система программируемых аппаратных взаимодействий предоставляет дополнительные возможности для самостоятельного программирования алгоритмов работы контроллера, что позволяет реализовывать специфические требования к системе управления доступом или использовать контроллеры вне рамок систем управления доступом, например, в системах управления зданием или в устройствах промышленной автоматики.

Описание возможностей системы программируемых аппаратных взаимодействий дано в п. 1.4.11.

В полном объёме функционал взаимодействий поддержан в контроллерах доступа Elsys-MB (кроме Elsys-MB-SM) и Elsys-NG-xx. Особенности настройки взаимодействий в модулях Elsys-IO/MB и Elsys-RM-16C описаны в п. 2.3.7, а особенности настройки взаимодействий в охранных контроллерах Elsys-MB-AC и Elsys-AC2 – в п. 2.3.8.

2.3.2 Настройка взаимодействий

Настройка взаимодействий выполняется в окне, появляющемся при выборе в дереве устройств узла «Взаимодействия» (см. Рисунок 64), и заключается в назначении команд по управлению одним устройством (объект управления) на события от другого устройства (источник события).

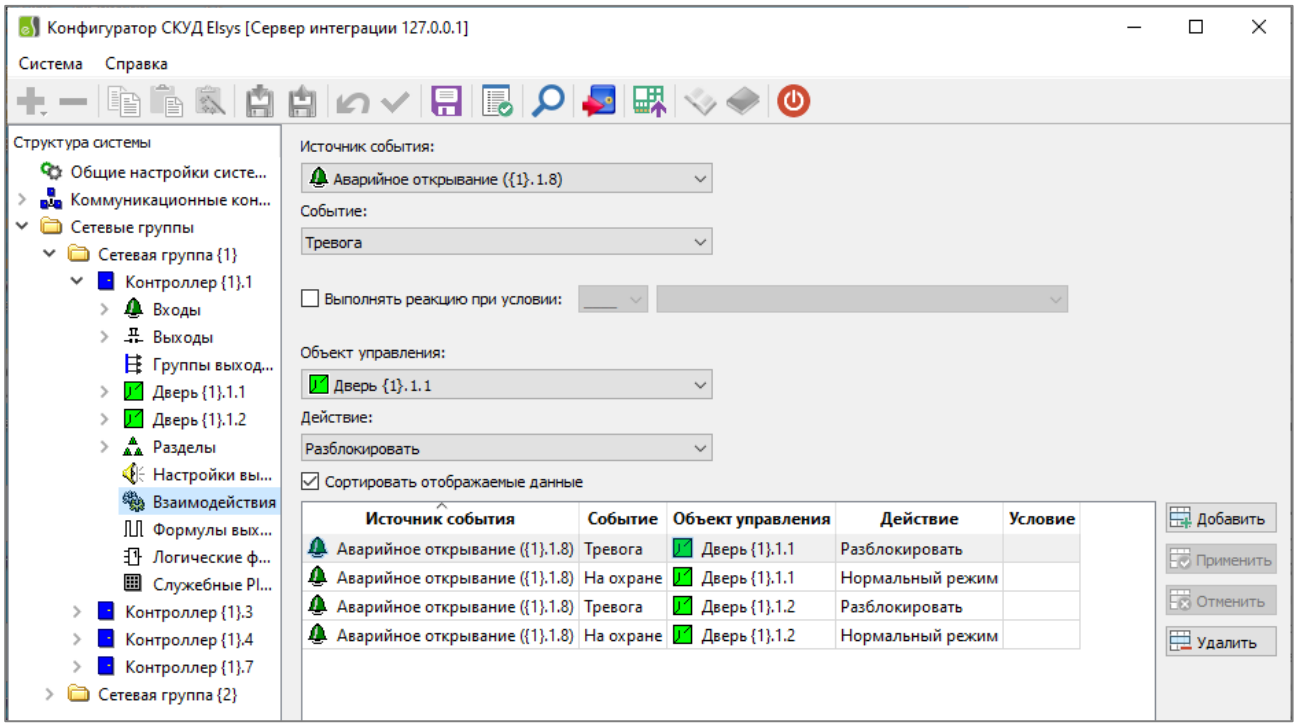

Рисунок 64. Окно настройки взаимодействий

Добавление и редактирование взаимодействий осуществляется кнопками в правой части окна настроек «Добавить», «Применить», «Отменить» и «Удалить».

Если события или управляющие действия имеют параметры (формула выхода, временной блок, время действия и др.), на экране отображаются элементы редактирования дополнительных параметров.

Чтобы задать дополнительное условие для выполнения реакции на событие, следует включить опцию «Выполнять реакцию при условии» и выбрать нужную логическую формулу (см. п. 2.3.4) в качестве условия, и, при необходимости, включить инверсию условия.

2.3.3 Настройка формул управления работой выходов

Формулы управления работой выходов описывают алгоритмы работы выходов контроллера, используемые во взаимодействиях в качестве параметра команды «Включить выход по формуле».

Настройка списка формул управления работой выходов происходит в окне настройки, которое становится доступным при выборе в дереве устройств элемента «Формулы выходов» (см. Рисунок 65).

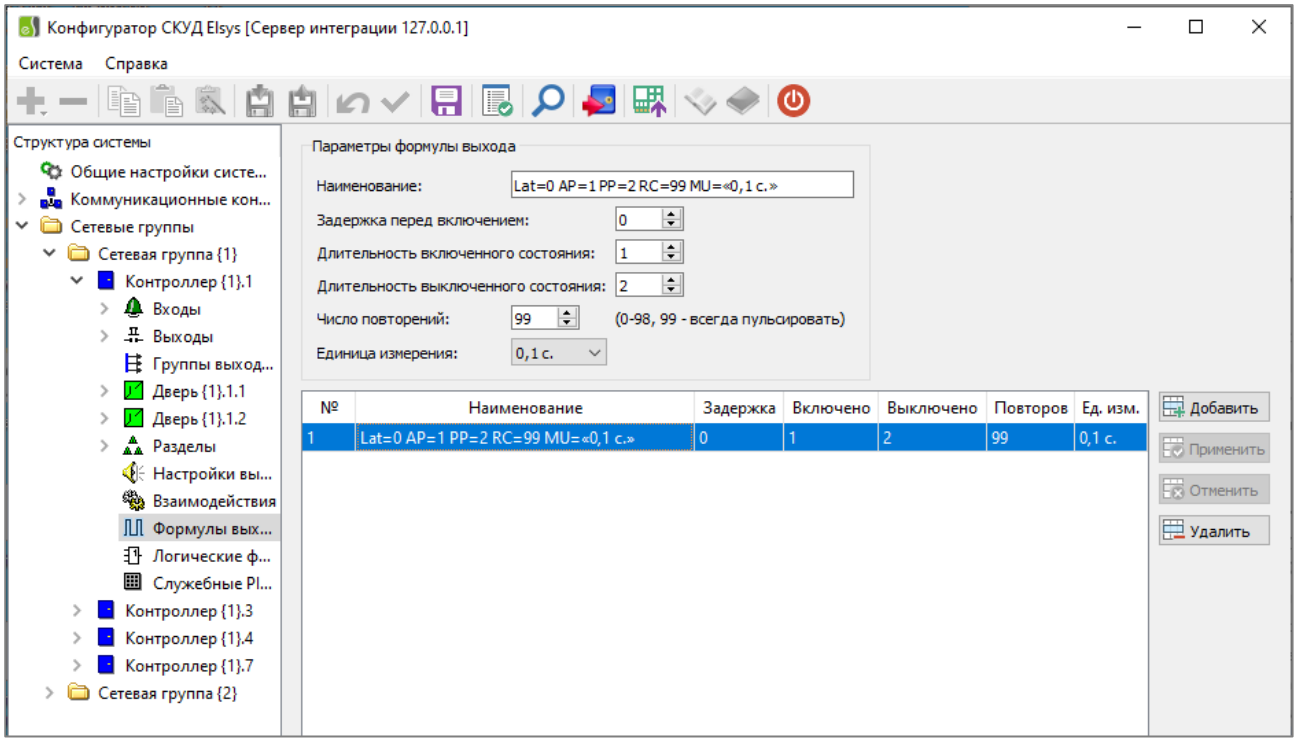

Рисунок 65. Окно настройки формул управления работой выходов

Название формул формируется автоматически и содержит полную информацию о формуле в следующем формате:

– «Lat» – задержка включения выхода,
– «AP» – длительность активной части периода (выход включен),
– «PP» – длительность пассивной части периода (выход выключен),
– «RC» – число пульсаций,
– «MU» – единица измерения времени для данной формулы.

Допустимые единицы измерения – 0,1 с, 1 с, 10 с, 1 мин, 10 мин

2.3.4 Настройка логических формул

Логическая формула – это логическое выражение, состоящее из последовательности логических условий, объединённых логическими

операциями «И», «ИЛИ», «ИСКЛЮЧАЮЩЕЕ ИЛИ», «НЕ». В качестве логических условий могут быть использованы состояния входов, выходов, групп выходов, временных блоков и логических формул. Для редактирования списка логических формул следует выбрать в дереве устройств пункт «Логические формулы», после чего в правой части экрана появится окно, изображённое на рисунке (см. Рисунок 66). Пользовательский интерфейс составления логической формулы позволяет включать в одну формулу до трёх условий, однако использование в качестве операндов других логических формул позволяет составлять многоэлементные логические формулы. Скобки в логическом выражении обеспечивают последовательное выполнение логических операций в порядке их расположения в окне редактирования (сверху вниз).

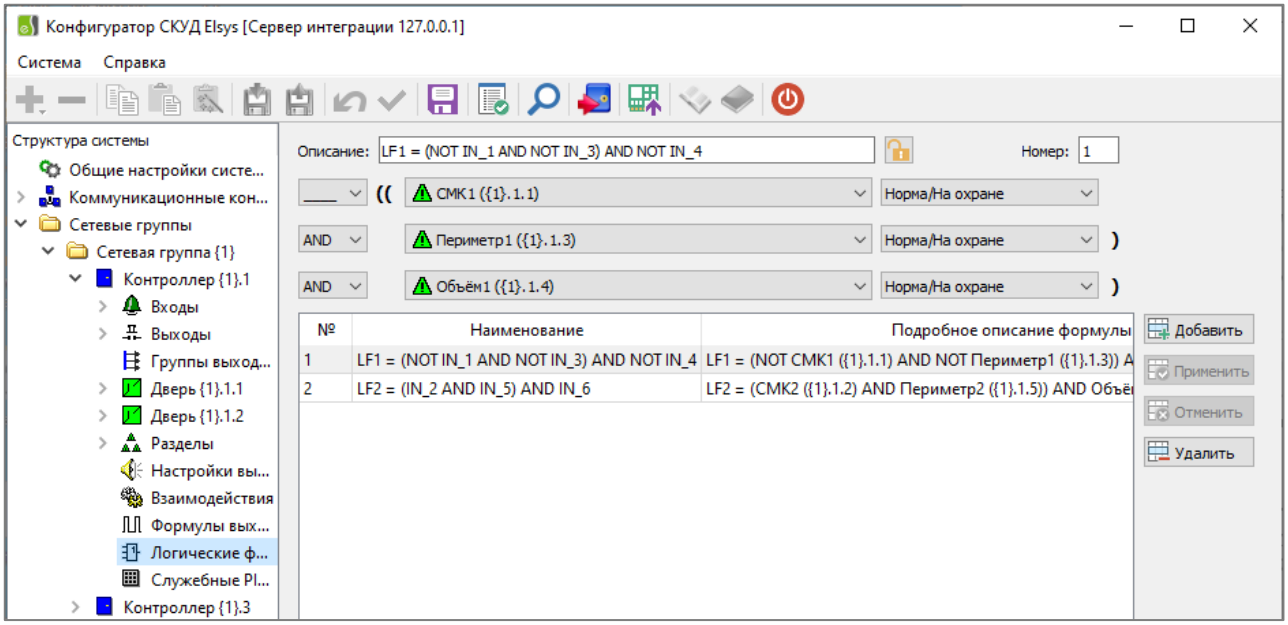

Рисунок 66. Окно настройки логических формул

Логические формулы могут являться источниками событий, при этом возможно назначение реакций на события «Активность логической формулы», «Неактивность логической формулы», либо использоваться в качестве условия выполнения реакции (см. Рисунок 67).

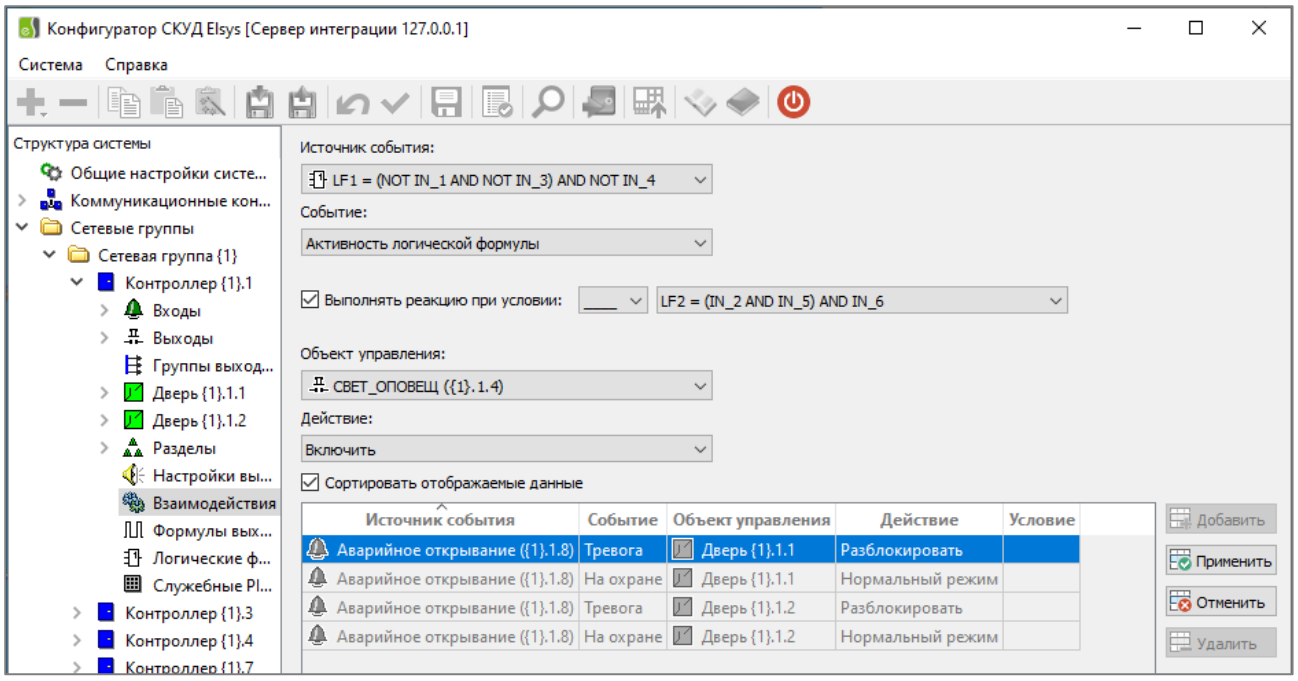

Рисунок 67. Настройка взаимодействий при использовании логических формул

Редактирование логических формул осуществляется аналогично редактированию взаимодействий. Элементами в верхней части окна задаются устройства, используемые в формуле, а также логические операции. Имя формулы формируется автоматически и может быть изменено. В списке логических формул, находящемся в нижней части окна, для каждой формулы представлено также её полное описание.

2.3.5 Настройка служебных PIN-кодов

В контроллерах предусмотрена возможность назначения реакций на ввод отдельных PIN-кодов, а также на совместное предъявление PIN-кода и карты доступа. В каждом контроллере может быть запрограммировано до 16 служебных PIN-кодов (паролей), причём ни один из этих кодов не должен совпадать ни с одним пользовательским PIN-кодом, а все пароли должны быть уникальными.

Для редактирования списка PIN-кодов следует выбрать узел «Служебные PIN-коды», относящийся к контроллеру, после чего в правой части экрана появится окно, изображённое на рисунке (Рисунок 68).

Добавление и редактирование PIN-кодов осуществляется кнопками, расположенными в правой части окна настройки (см. Рисунок 68).

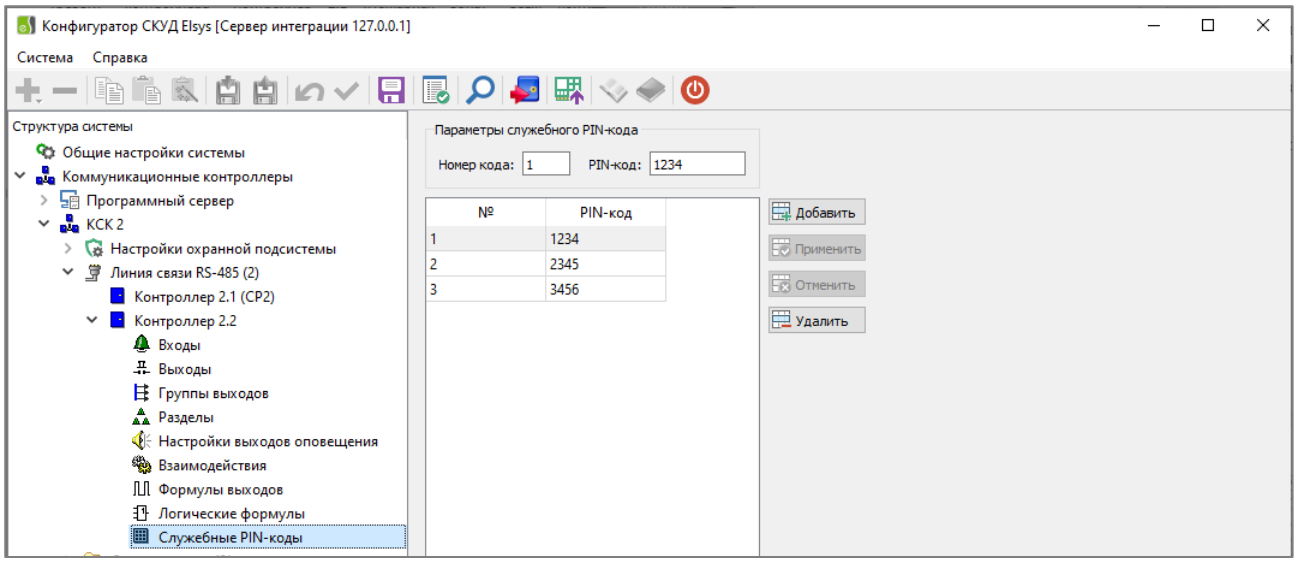

Рисунок 68. Окно настройки служебных PIN-кодов

Добавленные служебные PIN-коды могут использоваться во взаимодействиях в событиях «Ввод пароля (вх. сч./вых.сч.)», «Ввод пароля и предъявление карты (вх. сч./вых.сч.)» (см. Рисунок 69).

События, сопровождаемые предъявлением карты, регистрируются в протоколе, при этом каждое из них имеет 16 вариантов вида «Ввод PIN1 + PROX (вх. сч./вых.сч.)», «Ввод PIN2 + PROX (вх. сч. /вых.сч.)»…«Ввод PIN16 + PROX (вх. сч. /вых.сч.)».

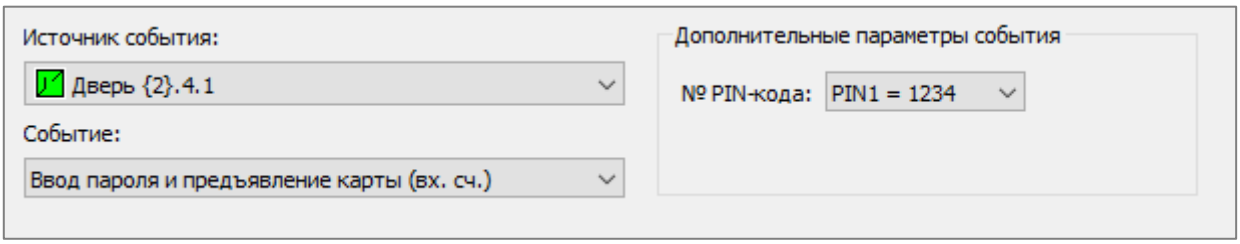

Рисунок 69. Пример применения PIN-кода в качестве источника события

Для пользователей, которым разрешено пользоваться служебными PIN-кодами, должна быть включена опция «Право ставить на охрану», в ином случае события типа «Ввод PINXX + PROX (..)» формироваться не будут.

2.3.6 Дополнительные сведения по настройке взаимодействий

2.3.6.1 Настройка счётчиков событий

Счётчики событий предназначены для подсчёта событий и выполнения реакций на изменение значения счётчика. Во взаимодействиях все события и

команды, относящиеся к работе со счётчиками, отнесены к устройству «Контроллер».

На любое событие могут быть назначены реакции:

– увеличить значение счётчика;
– уменьшить значение счётчика;
– установить значение счётчика.

Аппаратные реакции могут быть назначены на события:

– равенство счётчика значению;
– равенство счётчика значению после увеличения значения;
– равенство счётчика значению после уменьшения значения.

Счётчики могут принимать значения от 0 до 63. Значение счётчика циклически изменяется, то есть при уменьшении значения счётчика, равного нулю, новое значение будет 63, и наоборот, при увеличении значения счётчика, равного 63, новое значение будет 0.

На рисунке (Рисунок 70) приведён практический пример использования счётчиков событий. Для помещения, оборудованного двусторонней дверью, реализовано ограничение доступа (т. е. запрещён доступ всем, кроме имеющих привилегию прохода при ограничении доступа) при количестве людей в помещении более четырёх. Для подсчёта количества людей используются события «Штатный вход» и «Штатный выход». В полночь («Начало временного блока 3») и по включению питания счётчик обнуляется.

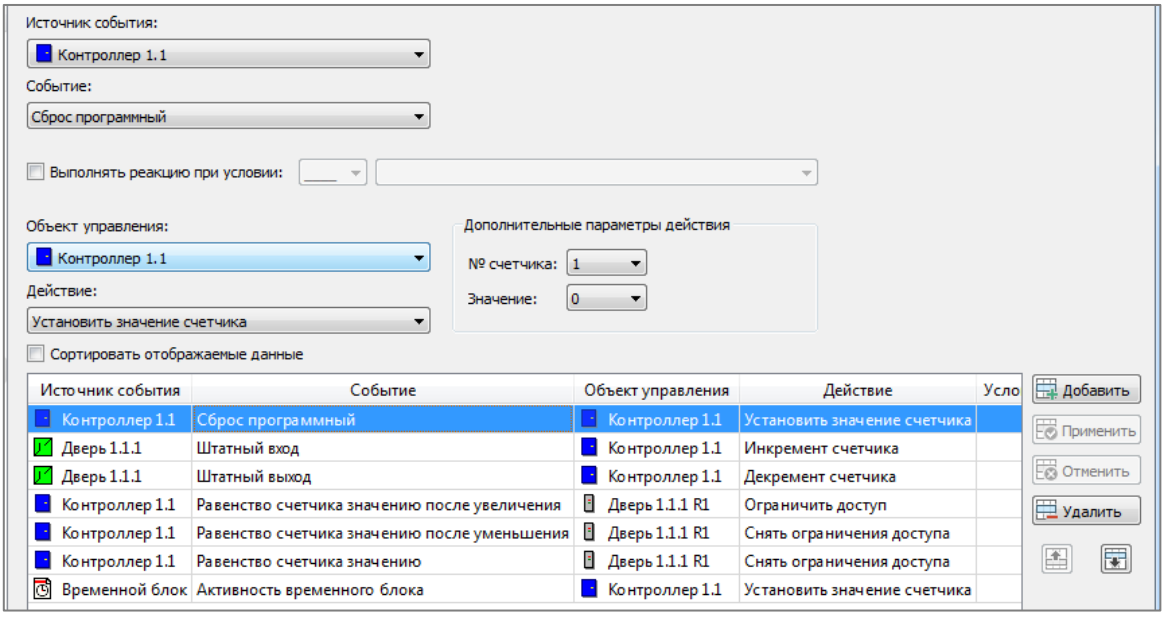

Рисунок 70. Пример настройки счётчиков событий

2.3.6.2 Настройка взаимодействий между контроллерами

В СКУД Elsys существует возможность настройки взаимодействий между контроллерами, а также назначения реакций на потерю и восстановление связи с отдельными контроллерами.

Взаимодействия между контроллерами функционируют в пределах единого информационного пространства, в котором должен быть настроен обмен данными между контроллерами и КСК (см. п. 2.2.7). В дополнение к описанным в п. 2.2.7 настройкам необходимо для КСК, обеспечивающих информационный обмен между контроллерами, включить опцию «Транслировать межконтроллерные взаимодействия в другие линии связи» (см. Рисунок 23).

Суть механизма, реализующего взаимодействия между контроллерами, в следующем. В качестве реакции на событие может быть назначено действие «Сформировать сообщение контроллерам» (см. Рисунок 71). Номер событий может быть задан в диапазоне 1 – 64, причём в качестве адресата могут быть выбраны либо все контроллеры, либо один из них. В свою очередь, на любое событие с заданным номером («Сообщение от контроллера») от любого контроллера (или от конкретного) могут быть назначены реакции (см. Рисунок 72).

Внимание! При отправке сообщения всем контроллерам, контроллер, от которого исходит сообщение, отправляемое сообщение не получит.

Кроме того, существует возможность назначения реакций на потерю связи:

- с выбранным контроллером;
- с любым из контроллеров (взаимодействия обрабатываются, если до этого была связь со всеми контроллерами);
- с КСК, участвующим в обмене (или с ПК, если контроллер подключен к COM-порту);

а также на восстановление связи:

- с выбранным контроллером;
- со всеми контроллерами;

– с КСК, участвующим в обмене (или с ПК, если контроллер подключен к COM-порту).

Практический пример использования взаимодействий между контроллерами – реализация аварийной разблокировки точек эвакуации при пожарной тревоге и возвращения их в нормальный режим по окончании тревоги – приведён на рисунках (Рисунок 71, Рисунок 72).

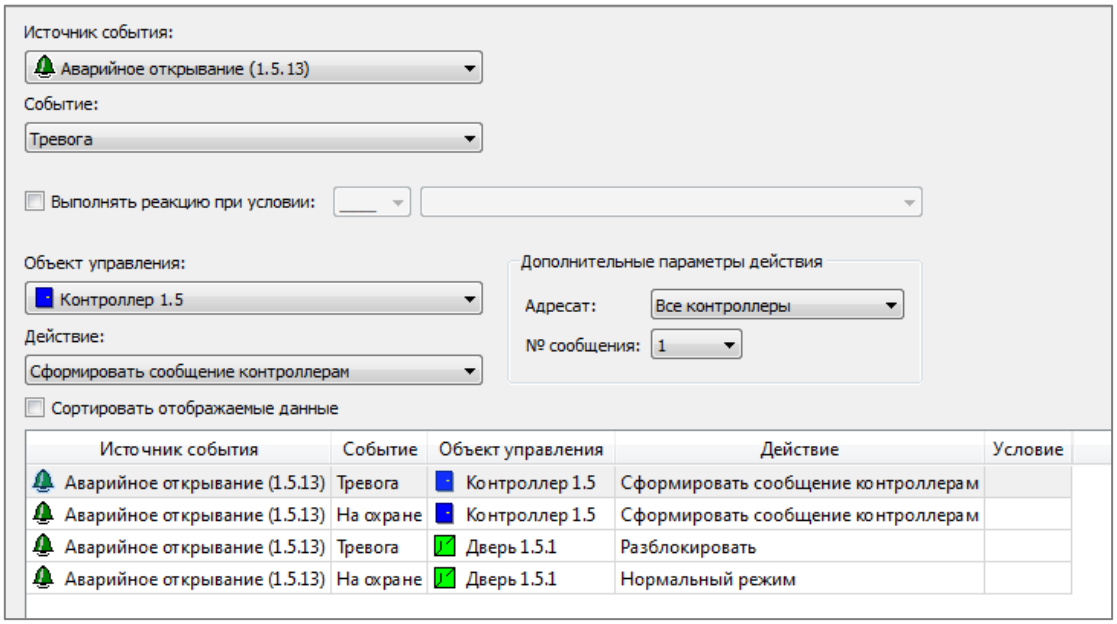

Рисунок 71. Настройка межконтроллерных сообщений

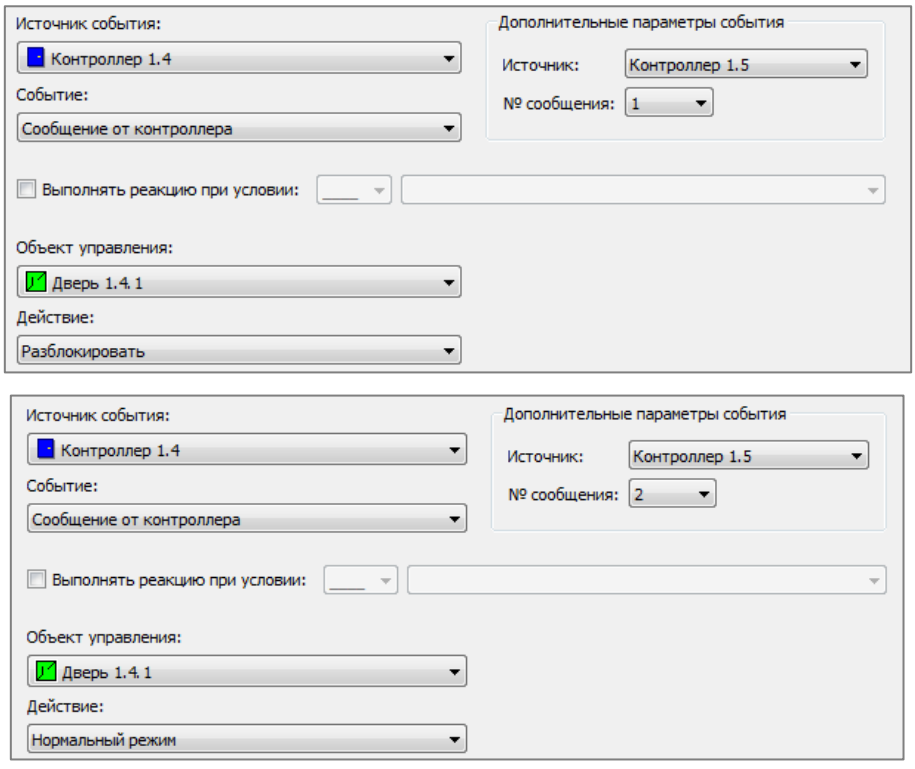

Рисунок 72. Настройка реакций на сообщения от других контроллеров

2.3.6.3 *Назначение реакций на предъявление карт доступа*

В контроллерах доступа могут быть назначены реакции на предъявление отдельных карт. В качестве служебной может быть назначена карта с любым номером, который необходимо ввести в шестнадцатеричном виде в окне редактирования взаимодействий (см. Рисунок 73). Всего во взаимодействиях в каждом контроллере могут участвовать не более 48 служебных карт.

Назначение реакций возможно на перечисленные ниже события точек доступа:

- штатное предъявление служебной карты входному считывателю;
- штатное предъявление служебной карты выходному считывателю;
- предъявление служебной карты входному считывателю;
- предъявление служебной карты выходному считывателю.

Первые два события обрабатываются, если полномочия разрешают доступ (с учётом анализа уровня доступа, временной зоны и зоны доступа), а последние два – при любом предъявлении карты.

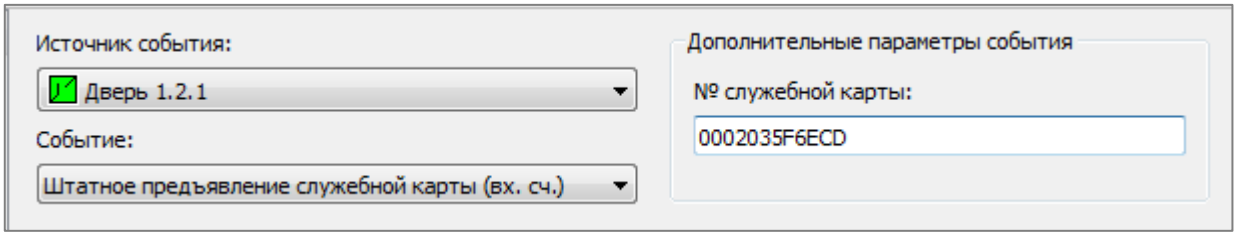

Рисунок 73. Пример настройки события предъявления конкретной карты

2.3.6.4 *Назначение реакций на удержание ключа/карты*

Возможность контроля нахождения карты доступа в зоне действия считывателя может быть реализована в контроллерах доступа только при подключении считывателей по интерфейсу Touch Memory, так как только в этом режиме считыватель непрерывно передаёт код карты, пока она находится в зоне действия считывателя.

Для использования режима контроля удержания карты необходимо выполнение следующих условий:

- считыватель должен быть подключен по интерфейсу Touch Memory;
- в свойствах контроллера настройка «Интерфейс считывателей» должна иметь значение «Touch Memory»;

– в свойствах выбранного считывателя должна быть включена настройка «Анализировать удержание ключа/карты»;
– должна быть включена дополнительная опция пропуска «Право ставить на охрану».

Если используется этот режим, кратковременное предъявление карты будет формировать событие «Предоставление доступа» (формируется в момент отпускания карты/ключа), а удержание свыше заданного времени будет интерпретироваться как удержание карты. Время, в течение которого необходимо удерживать карту или ключ для формирования события «Удержание карты/ключа», задаётся в настройках считывателя (вкладка «Дополнительные», опция «Интервал при постановке на охрану» см. Рисунок 55).

Если у выбранного считывателя назначен раздел для управления и индикации, удержание карты/ключа будет вызывать действие по управлению режимом охраны раздела (постановку на охрану или снятие с охраны). Если раздел для управления и индикации не назначен, при удержании карты или ключа будет сформировано событие «Удержание карты/ключа» (регистрируется в протоколе и может участвовать во взаимодействиях), а по окончании удержания – событие «Отпускание карты/ключа» (может участвовать во взаимодействиях, но не регистрируется в протоколе).

Одно из возможных применений использования описываемой возможности – ручное ограничение режима доступа в помещение (например, если в кабинете руководителя проходит совещание). Для реализации этой функции необходимо настроить взаимодействия, как показано на рисунке (Рисунок 74).

Источник события	Событие	Объект управления	Действие	Условие
Дверь 1.1.1	Удержание ключа/карты вх. сч.	Группа выходов 1.1.1	Инвертировать состояние выхода	
Группа выходов 1.1.1	Включение	Дверь 1.1.1 R1	Ограничить доступ	
Группа выходов 1.1.1	Выключение	Дверь 1.1.1 R1	Снять ограничения доступа	
Группа выходов 1.1.1	Включение	Выход 1.1.18 (инд. ограничения доступа)	Включить	
Группа выходов 1.1.1	Выключение	Выход 1.1.18 (инд. ограничения доступа)	Выключить	

Рисунок 74. Использование события «Удержание»
для реализации режима ограничения доступа

В конфигурацию контроллера добавлено вспомогательное устройство – группа выходов «Группа 1.1.1» (выходы включать в её состав не нужно). Каждое событие «Удержание карты» переключает состояние вспомогательной группы выходов. Если группа переходит в состояние «Включено», для считывателя включается режим ограничения доступа. При переходе группы в состояние «Выключено», считыватель переходит в обычный режим работы. Для сотрудников, которые должны всегда иметь право доступа в помещение, следует включить опцию «Проход в режиме ограничения доступа».

Ещё один пример применения контроля удержания карты – включение заданного выхода на время удержания карты (см. Рисунок 75). Эта функция может использоваться, например, для управления освещением в гостиничных номерах.

Источник события	Событие	Объект управления	Действие	Условие
Дверь 1.2.1	Удержание ключа/карты вх. сч.	Выход 1.2.4	Включить	
Дверь 1.2.1	Отпускание ключа/карты вх. сч.	Выход 1.2.4	Выключить	

Рисунок 75. Настройка взаимодействий
для включения выхода на время удержания карты

2.3.6.5 Настройка управления по временным расписаниям

Временные блоки с номерами 1 – 127 могут участвовать в качестве источников событий во взаимодействиях и в качестве операнда в логических формулах.

Внимание! Создание и настройку временных блоков следует выполнять в клиентском программном обеспечении. Для обеспечения загрузки временного блока в контроллер необходимо также создать уровень доступа, содержащий в качестве элементов считыватели контроллера с назначенным соответствующим временным блоком и пропуск, которому назначен этот уровень доступа.

Для настройки взаимодействий по временным расписаниям следует выбрать в качестве источника события узел «Временной блок», в качестве события – «Активность временного блока» или «Неактивность временного блока» и задать ему номер (см. Рисунок 76).

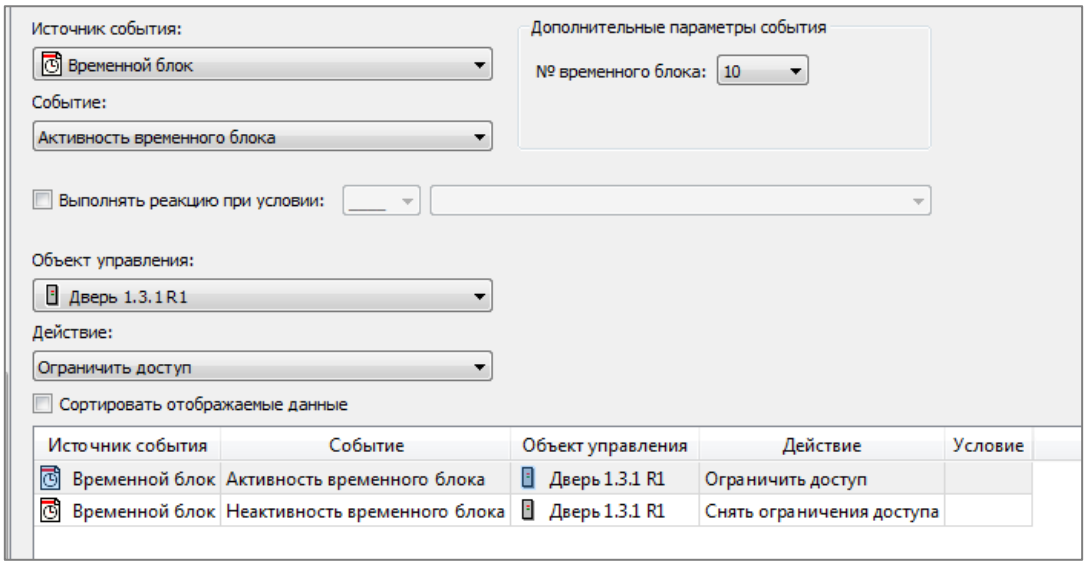

Рисунок 76. Использование временных блоков при настройке взаимодействий

Аналогичным образом настраивается использование временных блоков в логических формулах (см. Рисунок 77).

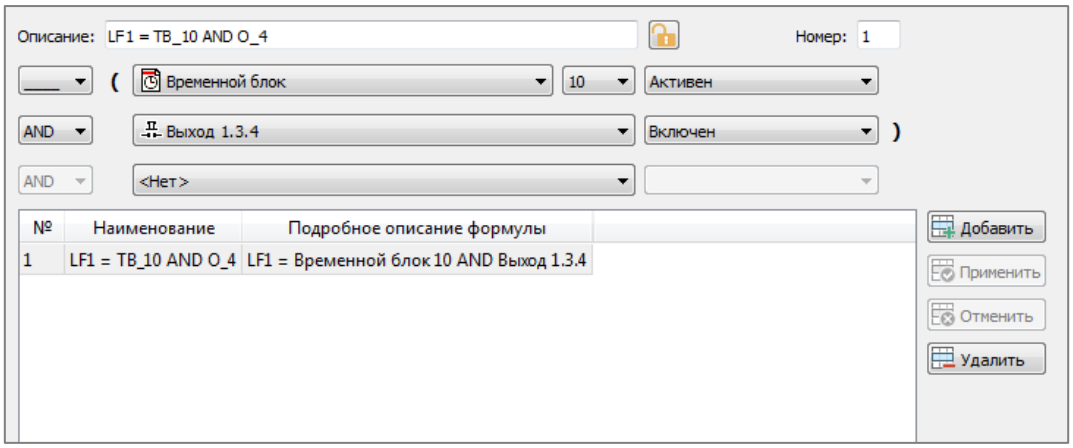

Рисунок 77. Использование временных блоков в логических формулах

2.3.6.6 Настройка функций, связанных с подсчётом персонала

В контроллерах доступа Elsys-MB (кроме Elsys-MB-SM), Elsys-NG-xx предусмотрена возможность ведения подсчёта персонала в областях контроля (зонах доступа), обслуживаемых каждым контроллером.

Внимание! Одновременная работа временного контроля последовательности прохода (см. п. 2.4.6.3) и функций подсчёта персонала в контроллерах не поддерживается!

В контроллерах Elsys-MB для работы этой функции необходимо выполнение следующих условий:

– наличие модуля расширения памяти;
– должна быть включена опция «Расширенные возможности настройки».

Внимание! Следует учитывать, что описываемые в настоящей главе функции подсчёта персонала и автоматическая постановка на охрану при выходе последнего сотрудника (см. документ «TCOC Elsys. Руководство по эксплуатации») работают и настраиваются независимо друг от друга.

Функция подсчёта персонала может быть включена для любой двусторонней точки доступа. Для использования этой функции необходимо включить опцию «Вести подсчёт количества персонала в областях контроля» (см. Рисунок 44, Рисунок 45, Рисунок 46).

Подсчёт персонала работает следующим образом. После каждого события «Штатный вход» или «Штатный выход» контроллер пересчитывает и обновляет общее число сотрудников, находящихся во внутренней зоне доступа. Подсчёт числа сотрудников, находящихся во внутренней зоне доступа, выполняется также для каждого из уровней доступа. Если включен глобальный контроль последовательности прохода, для подсчёта количества сотрудников используются также события от других контроллеров о перемещении пользователей.

При включенной функции подсчёта персонала формируются следующие события:

– «Штатный вход первого сотрудника»;
– «Штатный выход последнего сотрудника»;
– «Штатный вход первого сотрудника с заданным уровнем доступа»;
– «Штатный выход последнего сотрудника с заданным уровнем доступа».

Перечисленные события могут участвовать в аппаратных взаимодействиях. Если эти события необходимо регистрировать в протоколе, следует использовать опции точки доступа «Регистрировать вход первого и выход последнего» и «Регистрировать вход первого и выход последнего (для каждого уровня доступа)» (см. Рисунок 44, Рисунок 45, Рисунок 46).

Если необходимо назначить реакции на изменение количества персонала в помещении, следует задать связь точки доступа со счётчиком событий,

настроив реакцию на вспомогательное событие «Изменение количества персонала» или «Изменение количества персонала с заданным уровнем доступа», на которое должна быть назначена команда «Установить значение счётчика» (см. Рисунок 78).

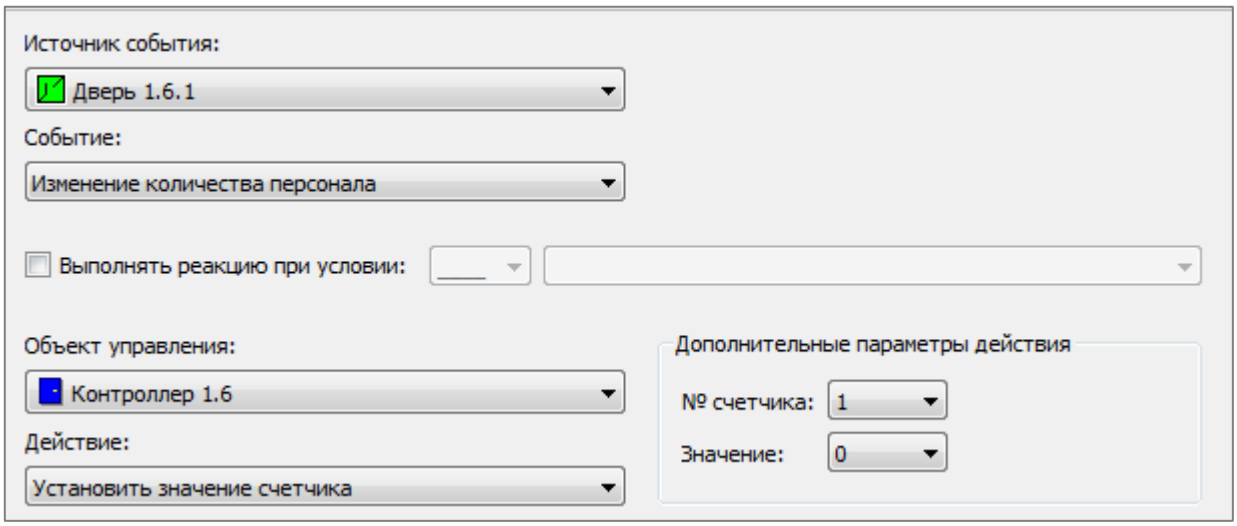

Рисунок 78. Настройка взаимодействий для подсчёта количества персонала

В отличие от других взаимодействий, это взаимодействие не выполняется, но обеспечивает автоматическую загрузку значения счётчика событий № 1 числовым значением количества персонала во внутренней зоне точки доступа. Устанавливаемое значение счётчика роли не играет. На вспомогательные события «Изменение количества персонала» и «Изменение количества персонала с заданным уровнем доступа» любые другие реакции назначены быть не могут – они выполняться не будут. Счётчик событий, назначенный таким образом для подсчёта персонала, может быть использован во взаимодействиях как источник событий (см. п. 2.3.6.1), что даёт дополнительные возможности для программирования логики работы.

После инициализации счётчик персонала находится в неопределённом состоянии, так как текущее местоположение сотрудников неизвестно. Поэтому, для корректной работы подсчёта персонала обязательно должен выполняться сброс счётчика персонала, например, по факту постановки помещения на охрану, при выполнении сброса или по другим событиям. Для установки текущего местоположения сотрудников в состояние «Внешняя зона» (соответствует состоянию, при котором во внутренней зоне никого нет) предусмотрены команды, выполняемые через взаимодействия (объект

управления – контроллер) – «Сбросить счётчик персонала» и «Сбросить счётчик персонала для УД» (см. Рисунок 79).

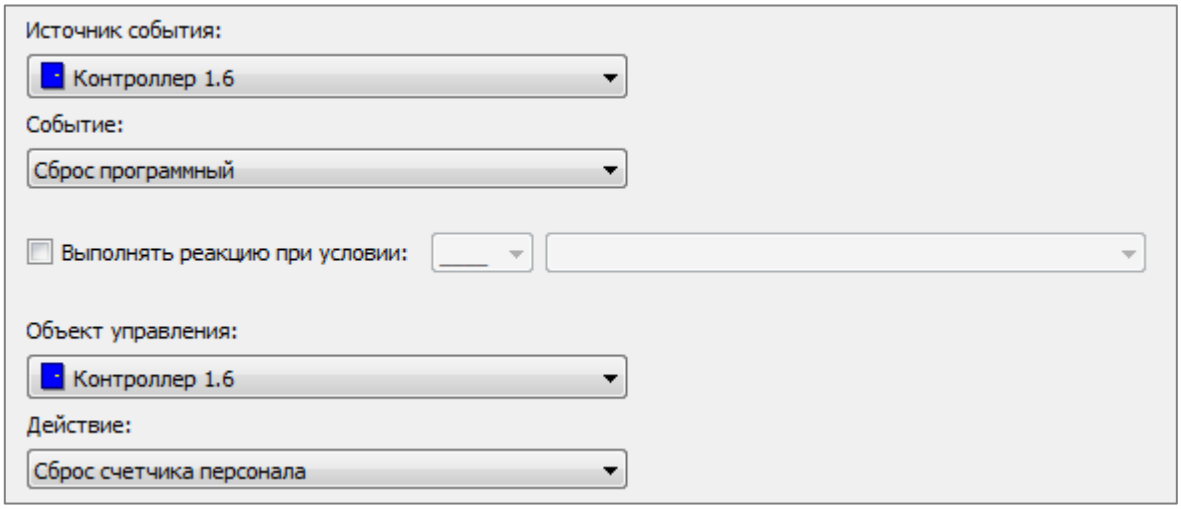

Рисунок 79. Настройка взаимодействий для сброса счётчика персонала

2.3.7 Особенности настройки взаимодействий в модулях Elsys-IO/MB и релейных модулях Elsys-RM-16C

Логические формулы и служебные PIN-коды в модулях Elsys-IO/MB и релейных модулях Elsys-RM-16C не поддерживаются.

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

В качестве источников событий могут быть:

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

2.3.8 Особенности настройки взаимодействий в охранных контроллерах Elsys-AC2 и Elsys-MB-AC

Логические формулы и служебные PIN-коды в охранных контроллерах Elsys-AC2 и Elsys-MB-AC не поддерживаются.

В качестве источников событий могут быть использованы следующие устройства:

- контроллер (событие «Сброс»);
- другие контроллеры (события № 1 – 64, «Потеря/восстановление связи»);

– входы;
– разделы.

В качестве объектов управления могут быть использованы следующие устройства:

– контроллер (команда «Сформировать сообщение контроллерам» с номером 1 – 64, для настройки межконтроллерных взаимодействий);
– выход;
– раздел;
– вход (при условии, что он не входит в разделы).

2.4 Настройка контроля последовательности прохода

Описание работы контроля последовательности прохода дано в п. 1.4.7.

2.4.1 Порядок настройки контроля последовательности прохода

В оборудовании СКУД Elsys поддерживаются следующие режимы контроля последовательности прохода (antipassback):

– локальный;
– глобальный аппаратный;
– глобальный программный.

Для настройки контроля последовательности прохода необходимо:

– выполнить настройки оборудования, в зависимости от используемого режима, в соответствии с пунктами 2.4.2, 2.4.3 или 2.4.4;
– настроить, при необходимости, дополнительные опции контроля последовательности прохода (см. п. 2.4.6);
– выполнить инициализацию оборудования из конфигуратора;

Если используется глобальный контроль последовательности прохода, необходимо:

– выполнить в клиентском программном обеспечении настройку зон доступа (см. п. 2.4.5; для обозначения зон доступа в клиентском программном обеспечении могут также использоваться термины «Область контроля» и «Территория»);
– выполнить инициализацию зон доступа в клиентском программном обеспечении.

2.4.2 Настройка локального контроля последовательности прохода

Настройка локального контроля последовательности прохода заключается в выборе соответствующего пункта на вкладке «Контроль последовательности прохода» контроллера доступа (см. Рисунок 80).

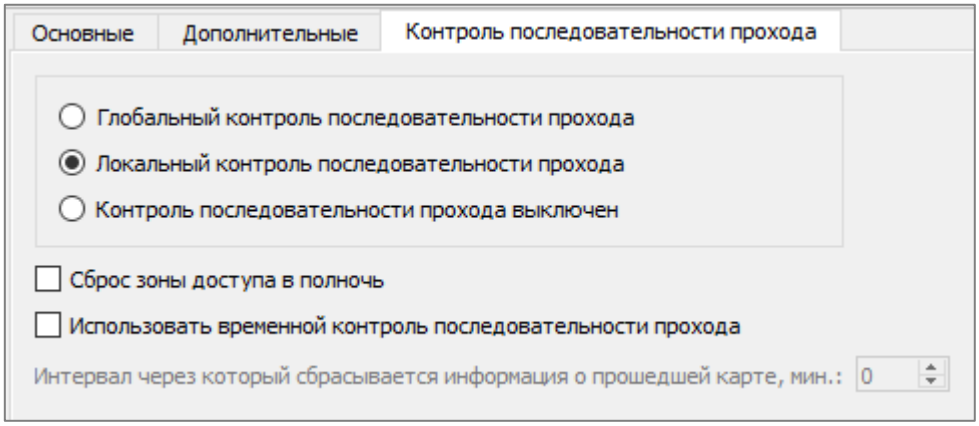

Рисунок 80. Вкладка настройки контроля последовательности прохода

В режиме локального контроля последовательности прохода контроллер будет обслуживать две зоны доступа – входную и выходную. Конфигурировать зоны доступа не требуется.

2.4.3 Настройка глобального аппаратного контроля последовательности прохода

Для настройки глобального аппаратного контроля последовательности прохода необходимо обеспечить обмен данными между контроллерами в едином информационном пространстве, для чего следует выполнить настройки в соответствии с п. 2.2.7.

На вкладке «Контроль последовательности прохода» свойств контроллера (см. Рисунок 80) следует включить настройку «Глобальный контроль последовательности прохода».

Также предусмотрена возможность группового включения настройки «Глобальный контроль последовательности прохода»:

– во всех контроллерах системы кнопкой «Включить antipassback/межконтроллерный обмен во всех контроллерах» в окне основных настроек системы (см. Рисунок 5);
– во всех контроллерах линии связи RS-485 кнопкой «Включить глобальный antipassback в линии связи» (см. Рисунок 25);

– во всех контроллерах сетевой группы кнопкой «Включить глобальный antipassback в сетевой группе» (см. Рисунок 29).

При выполнении этих групповых операций вместе с включением глобального контроля последовательности прохода будет выполнено включение необходимых режимов межконтроллерного обмена между КСК, в линиях связи и сетевых группах.

2.4.4 Настройка глобального программного контроля последовательности прохода

Для настройки глобального программного контроля последовательности прохода необходимо включить глобальный antipassback во всех контроллерах, где это необходимо, в соответствии с п. 2.4.3. Настройки, задающие режимы обмена между КСК, в линиях связи RS-485 и сетевых группах, на работу программного контроля последовательности прохода не влияют.

Для включения программного контроля последовательности прохода следует включить опцию «Программный контроль последовательности прохода» в окне основных настроек системы (см. Рисунок 5).

Настройка «Время ожидания восстановления связи в областях контроля» (значение по умолчанию – 60 с; диапазон значений 1 – 14400 с) задаёт максимально допустимое время нарушения связи с контроллерами, участвующими в программном контроле последовательности прохода. Без необходимости эту настройку изменять не следует.

Глобальный программный контроль последовательности прохода поддерживается в контроллерах доступа Elsys-NG-800 (начиная с версии прошивки 4.13), Elsys-NG-1000 (начиная с версии прошивки 5.05), Elsys-NG-200 (начиная с версии прошивки 3.10), Elsys-MB (начиная с версии прошивки 2.79). Контроллеры, участвующие в программном контроле последовательности прохода, могут опрашиваться сервером интеграции напрямую или через КСК Elsys-MB-Net II (с версией прошивки не ниже 3.15), КСК Elsys-NG-Net II (с версией прошивки не ниже 5.02).

2.4.5 Настройка зон доступа

Настройка зон доступа выполняется в клиентском программном обеспечении (см. Рисунок 81).

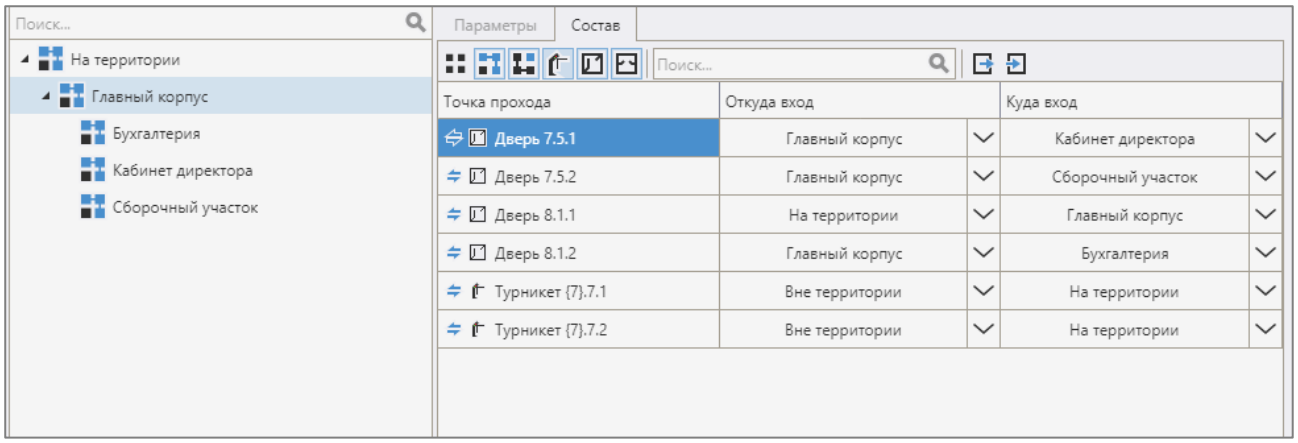

Рисунок 81. Окно настройки зон доступа

Настройка заключается в создании списка зон доступа и задании для точек доступа, участвующих в глобальном контроле последовательности прохода, зон доступа со стороны входного (колонка «Откуда вход») и со стороны выходного (колонка «Куда вход») считывателей точки доступа.

Редактирование зон доступа описано в руководстве администратора клиентского программного обеспечения. Вид окна настройки зон доступа может отличаться в зависимости от версии программного обеспечения.

2.4.6 Дополнительные настройки

2.4.6.1 Мягкий antipasssback

Если при использовании контроля последовательности прохода необходимо, регистрируя нарушение, автоматически предоставлять доступ, следует в свойствах считывателей на вкладке «Дополнительные» включить настройку «Предоставлять доступ при нарушении зоны доступа» (см. Рисунок 55).

2.4.6.2 Опция «Сброс в полночь»

Опция «Сброс в полночь» (см. Рисунок 80) обеспечивает сброс в ноль часов ноль минут информации о текущем местоположении всех сотрудников.

2.4.6.3 Временной antipassback

Внимание! Одновременная работа временного контроля последовательности прохода и функций подсчёта персонала (см. п. 2.3.6.6) в контроллерах не поддерживается!

Временной antipassback поддерживается в контроллерах Elsys-MB (при наличии установленного модуля расширения памяти) и в Elsys-NG-xx.

Временной antipassback настраивается путём выбора в окне настроек контроля последовательности прохода контроллера (см. Рисунок 80) опции «Использовать временной контроль последовательности прохода» и задании в поле «Интервал, через который сбрасывается информация о прошедшей карте», времени, спустя которое (диапазон значений 1 – 2047 минут) будет сброшена информация о текущей зоне доступа.

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

2.4.6.4 Усиленный antipassback

Опция «Усиленный antipassback» устанавливается в окне настройки сетевой группы (см. Рисунок 29) или линии связи RS-485 (см. Рисунок 25) и распространяется на все контроллеры сетевой группы или линии связи, где используется глобальный контроль последовательности прохода.

2.4.6.5 Опция «Не проверять исправность областей контроля»

Опция «Не проверять исправность областей контроля» определяет алгоритм работы функции antipassback при потерях связи с контроллерами.

Опция устанавливается в окне настройки сетевой группы (см. Рисунок 29) или линии связи RS-485 (см. Рисунок 25) и распространяется на все контроллеры сетевой группы или линии связи, где используется глобальный контроль последовательности прохода.

Если настройка выключена, все контроллеры непрерывно анализируют исправность обслуживаемых ими областей контроля. При потере связи с хотя бы одним контроллером, который обслуживает область контроля, antipassback прекращает работать и для всех сотрудников выполняется сброс текущего местоположения. Этот механизм предотвращает возможные необоснованные отказы в доступе, если из-за нарушений связи не все контроллеры получают информацию о текущем местоположении сотрудников.

Если настройка «Не проверять исправность областей контроля» включена, сброс текущего местоположения пользователей при нарушениях

связи не выполняется. Тем самым обеспечивается сохранение работоспособности функции antipassback при кратковременных и длительных нарушениях связи, однако становятся возможными необоснованные отказы в доступе.

2.5 Настройка специальных режимов работы

2.5.1 Двойная идентификация (PIN-код + карта)

Двойная идентификация пользователей возможна при использовании считывателей, имеющих встроенную клавиатуру.

Для обеспечения работы двойной идентификации необходимо выполнить ряд настроек:

- в окне основных настроек контроллера доступа включить опцию «Использовать PIN-коды» и задать интерфейс подключения считывателей, поддерживающий возможность передачи PIN-кодов в контроллер (Wiegand, ESDP, ESDP защищённый);
- в окне дополнительных настроек выбрать в выпадающем списке «Параметры ввода PIN-кода» способ завершения ввода PIN-кода (ввод символа «*» или «#»);
- в окне основных настроек считывателя (см. п. 2.2.12.1, Рисунок 54) задать тип используемого устройства «Считыватель и клавиатура»;
- если предполагается использование режима «Доступ под принуждением», следует включить в свойствах считывателя соответствующую настройку;
- выполнить настройку считывателя в соответствии с его эксплуатационной документацией.

В клиентском программном обеспечении в модуле «Бюро пропусков» необходимо для каждого пользователя задать PIN-код.

Если для конкретного пользователя PIN-код не задан либо включена дополнительная опция пропуска «Доступ только по карте», для предоставления доступа будет достаточно только предъявления карты.

2.5.2 Доступ с подтверждением картой

Доступ с подтверждением картой предназначен для предоставления доступа определенным категориям пользователей СКУД только в сопровождении лиц, у которых есть полномочия подтверждать доступ.

Для обеспечения работоспособности режима доступа с подтверждением картой необходимо убедиться, что:

– в окне основных настроек считывателя (см. Рисунок 54), где используется этот режим, отключены все полномочия дежурного оператора;
– в окне дополнительных настроек считывателя (см. Рисунок 55) в настройке «Интервал при предъявлении нескольких карт» правильно указан временной промежуток, в течение которого будет ожидаться предъявление карты, подтверждающей доступ.

На считывателях контроллера, где режим «Доступ с подтверждением» не нужен, необходимо включить на вкладке «Дополнительные» настройку «Игнорировать опцию пропуска «Доступ с подтверждением» (см. Рисунок 55).

Для корректной работы данного режима для лиц, которым требуется подтверждать доступ, должны быть заданы полномочия «Доступ с подтверждением» (см. Рисунок 82), а для лиц, которые должны подтверждать доступ – полномочия «Право подтверждать доступ» (см. Рисунок 83).

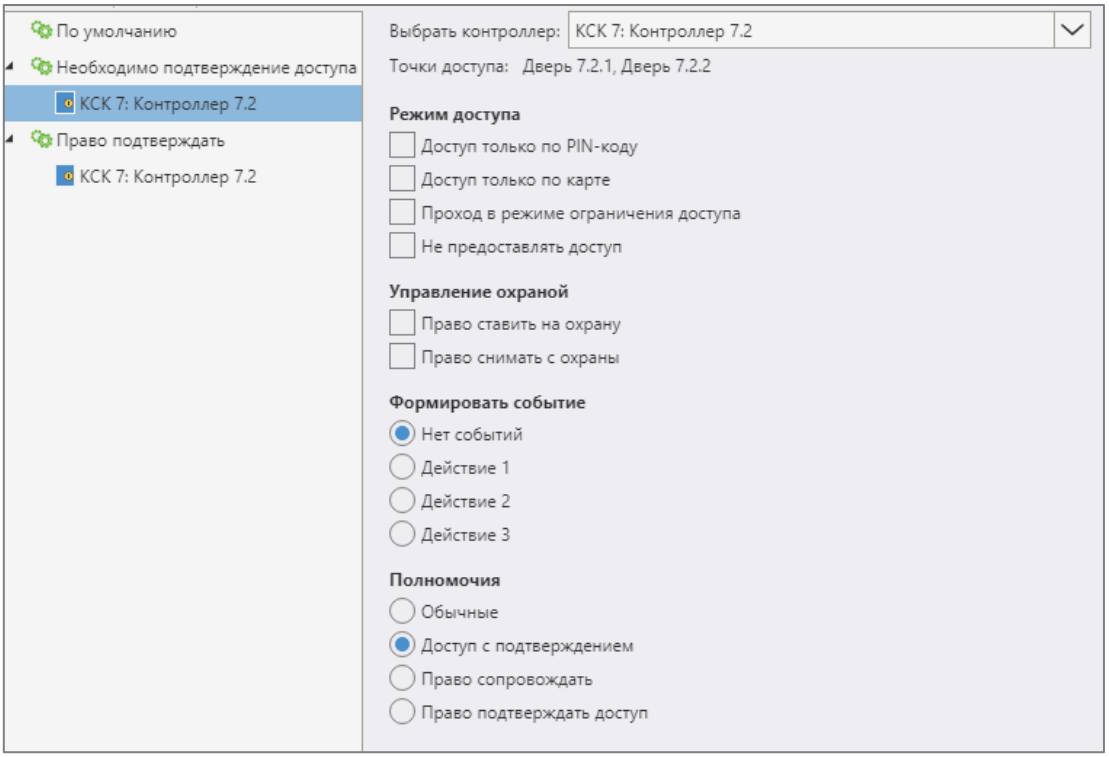

Рисунок 82. Настройка полномочий «Доступ с подтверждением»

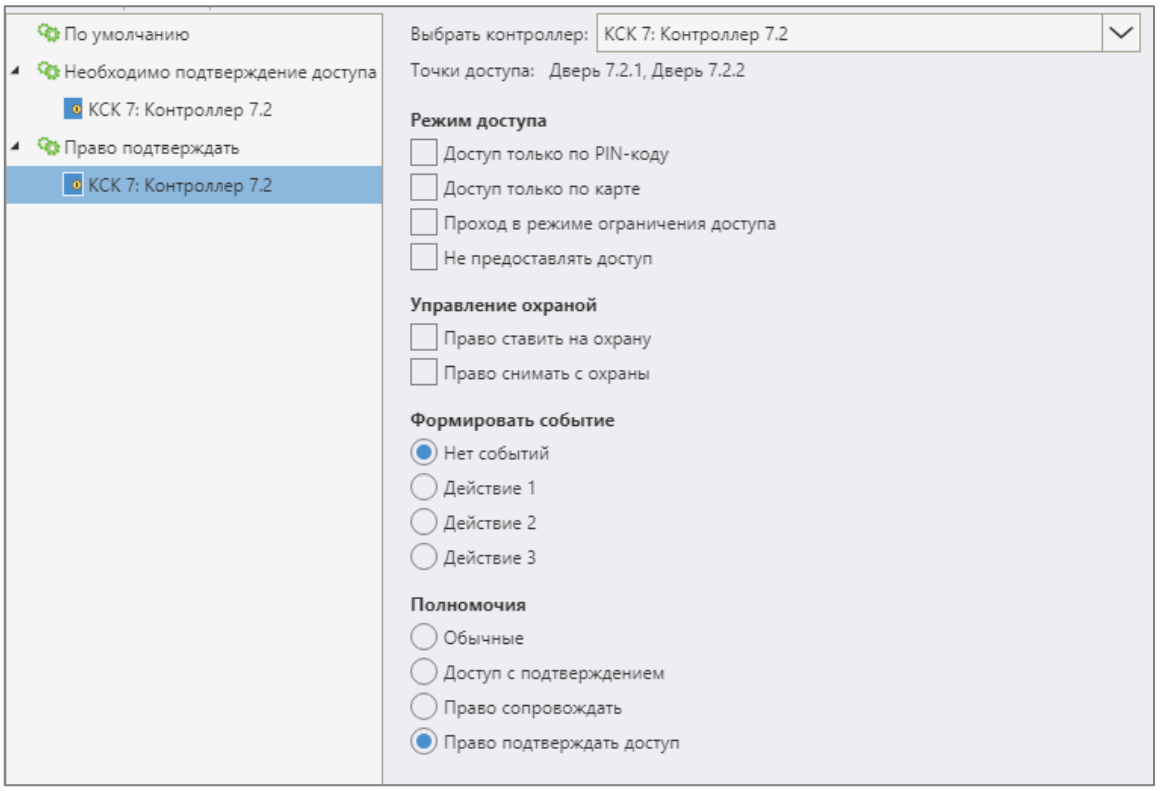

Рисунок 83. Настройка полномочий «Право подтверждать доступ»

Подробно настройка дополнительных полномочий пользователей описана в руководстве администратора на управляющее программное обеспечение.

2.5.3 Доступ с подтверждением кнопкой

Доступ с подтверждением кнопкой предназначен для предоставления доступа определенным категориям пользователей СКУД только с подтверждением дежурного оператора.

Для настройки этого режима необходимо в окне основных настроек считывателя (см. п. 2.2.12.1, Рисунок 54) выбрать опцию «Подтверждать доступ для карт с полномочиями «Доступ с подтверждением» и выбрать входы, к которым подключаются кнопки подтверждения доступа и отказа в доступе в выпадающих списках «Вход для подтверждения доступа» и «Вход для отказа в доступе».

Для лиц, которым требуется подтверждение доступа, необходимо установить дополнительные настройки, включив опцию «Доступ с подтверждением» (см. Рисунок 82).

На считывателях контроллера, где режим «Доступ с подтверждением» не нужен, необходимо включить на вкладке «Дополнительные» настройку «Игнорировать опцию пропуска «Доступ с подтверждением» (см. Рисунок 55).

Время ожидания подтверждения доступа кнопкой фиксировано и составляет 60 с.

2.5.4 Доступ с подтверждением из клиентского программного обеспечения

Команды подтверждения доступа или отказа в доступе могут быть сформированы как на аппаратном уровне (с помощью кнопок, подключенным к соответствующим входам, заданным в настройках считывателя), так и программно, путём передачи команды контроллеру из клиентского программного обеспечения.

Для настройки режима подтверждения доступа из клиентского программного обеспечения необходимо выполнить настройки в соответствии с п. 2.5.3.

Оба способа подтверждения (с использованием кнопок и с использованием команд, передаваемых из клиентского ПО) могут использоваться одновременно.

3 Инициализация оборудования

3.1 Инициализация настроек оборудования

Для инициализации настроек оборудования предназначено окно управления сервером интеграции (см. Рисунок 84), вызываемое по нажатию кнопки на панели быстрого доступа конфигуратора оборудования СКУД Elsys (см. Рисунок 6).

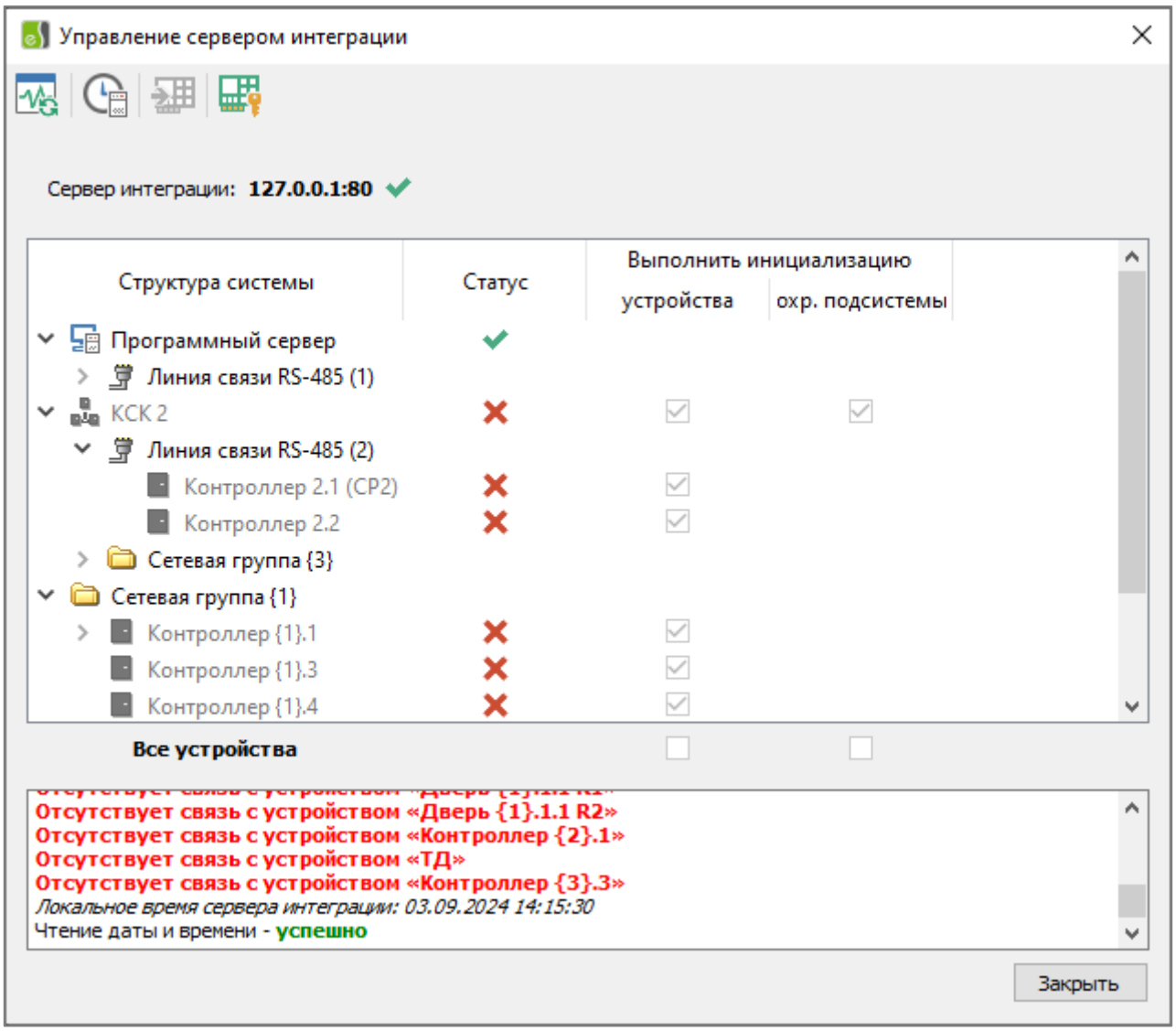

Рисунок 84. Форма управления сервером интеграции

В средней части окна управления сервером интеграции расположена таблица, содержащая список всех КСК, линий связи, контроллеров и считывателей ESDP, сохранённых в текущей конфигурации.

Колонка «Статус» отображает значок, соответствующий текущему состоянию связи конфигуратора с сервером интеграции и сервера интеграции с

устройствами системы (– есть подключение, – подключение отсутствует). Следующие колонки содержат элементы управления списком инициализируемых устройств. Флаги инициализации выставляются автоматически при наличии каких-либо изменений, внесённых в конфигурацию устройств или охранной подсистемы, с момента последней инициализации. При необходимости можно скорректировать список инициализируемых устройств.

Для загрузки настроек в контроллеры требуется нажать кнопку , которая отвечает за запуск процедуры инициализации оборудования и охранной подсистемы.

Процесс инициализации оборудования отображается в окне вывода информационных сообщений. Если в этом процессе произошла ошибка, то процедура инициализации немедленно прекращается и выводятся сообщения об ошибке.

Подробная информация о процедуре инициализации приведена в документе «Конфигуратор СКУД Elsys. Руководство пользователя».

3.2 Инициализация полномочий пользователей и зон доступа

Все изменения в базе данных пропусков (пропуска, уровни доступа, временные зоны, праздники, группы управления охраной) и зон доступа загружаются в контроллеры автоматически, при этом инициализация обычно не требуется. При кратковременных потерях связи автоматическую загрузку этих данных в оборудование обеспечивает механизм гарантированной доставки, реализованный в клиентском программном обеспечении.

Инициализацию полномочий пользователей подсистемы и конфигурации зон доступа требуется выполнять в следующих случаях:

- при начальной настройке оборудования;
- после очистки конфигурации контроллеров;
- после перенастройки распределения памяти между картами и событиями в настройках контроллера;
- после продолжительной (более часа) потери связи с отдельными контроллерами;
- в иных случаях, если обнаружено несоответствие числовых характеристик, сообщаемых оборудованием, с ожидаемыми.

Инициализация полномочий пользователей СКУД и охранной подсистемы, а также инициализация зон доступа, выполняемые из клиентского программного обеспечения, описаны в руководстве администратора на клиентское программное обеспечение.

4 Обновление прошивок оборудования

4.1 Обновление прошивок КСК и контроллеров

В автономном конфигураторе предусмотрено удалённое обновление прошивок подключенных устройств.

Внимание! Для обновления прошивок контроллеров Elsys-NG-1000, КСК Elsys-NG-Net II и совместимых с ними необходимо использовать специальную утилиту FtpUpdateUtility, поставляемую производителем оборудования. Процедура обновления описана в п. 4.3.

Для обновления прошивок предназначена специальная форма (см. Рисунок 84), вызываемая по нажатию кнопки на панели быстрого доступа конфигуратора оборудования СКУД Elsys (см. Рисунок 6).

Процесс удалённого обновления прошивки состоит из следующих этапов:

- выгрузка прошивки на сервер интеграции, проверка выгруженной прошивки;
- выбор линии связи и формирование списка устройств для удалённого обновления прошивки;
- запуск процесса загрузки прошивки в выбранные устройства.

Для выгрузки прошивки на сервер интеграции необходимо указать корректный файл с прошивкой устройства Elsys в диалоге выбора, отображаемом при нажатии кнопки . Данный файл в процессе выгрузки проверяется сервером интеграции. Результат проверки отображается в соответствующих информационных полях формы (статус выгрузки, тип устройства и версия прошивки).

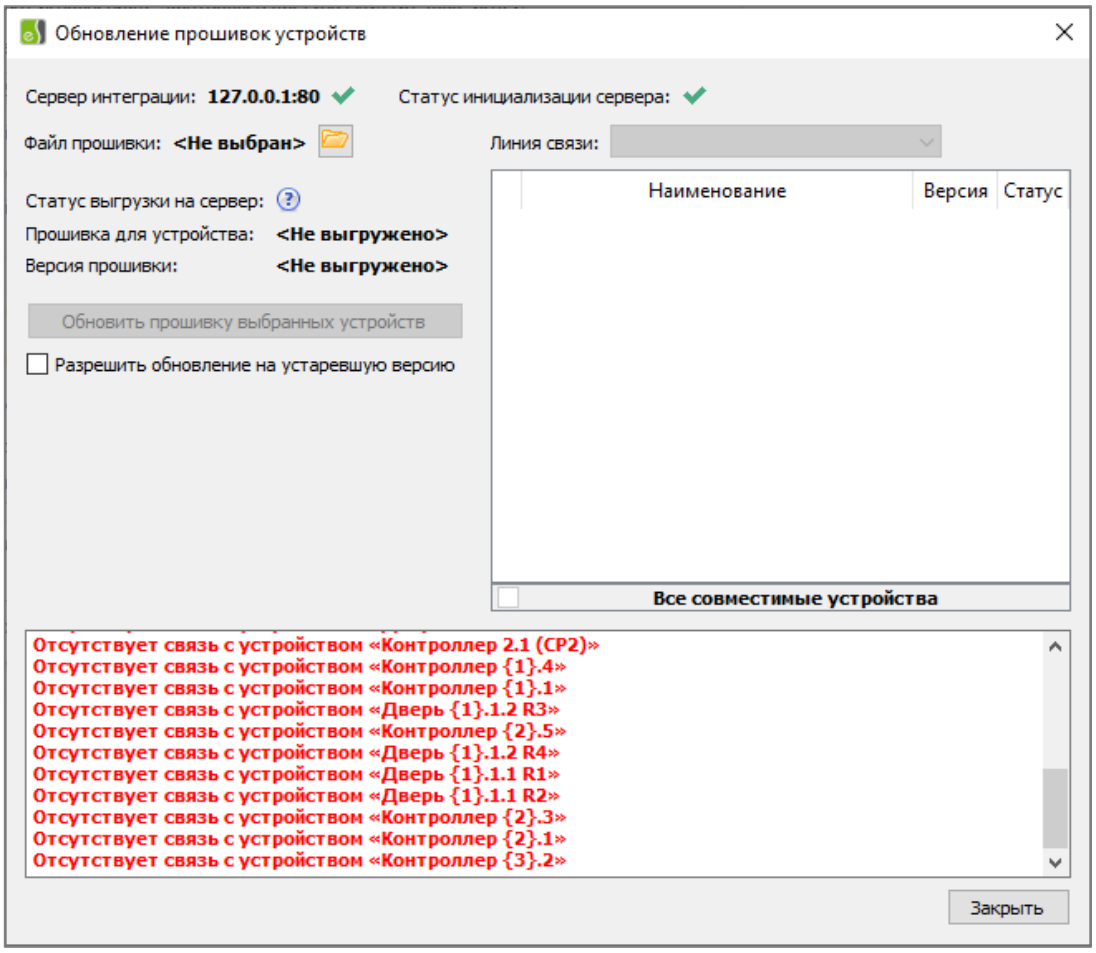

Рисунок 85. Форма управления процессом обновления прошивок устройств

Результатом успешной проверки прошивки будет отображение в выпадающем списке всех линий связи, среди которых будут доступны только те, в которые подключены устройства совместимые с прошивкой для обновления. Если выгружена прошивка КСК, выбор линии связи будет не доступен, а в списке устройств будут отображаться все доступные КСК.

При формировании списка устройств для обновления пользователю доступны те, с которыми присутствует связь и текущая прошивка старше загружаемой, при этом присутствует возможность обновить прошивку на более раннюю, выбрав опцию «Разрешить обновление на устаревшую версию».

После формирования списка устройств для обновления пользователю требуется осуществить загрузку прошивки в выбранные контроллеры нажатием кнопки «Обновить прошивку выбранных устройств». При успешном завершении у обновляемых контроллеров в конфигурации автоматически обновится версия прошивки.

Более подробная информация об удалённом обновлении прошивок устройств приведена в документе «Конфигуратор СКУД Elsys. Руководство пользователя».

4.2 Обновление прошивок устройств ESDP

Обновление прошивок устройств ESDP осуществляется аналогично обновлению прошивок КСК и контроллеров.

Чтобы устройство ESDP было доступно для обновления после выбора файла прошивки, его тип, указанный в конфигурации, должен совпадать с типом, указанным в файле прошивки. Если контроллер, к которому подключено устройство ESDP, опрашивается через КСК, то его версия должна быть актуальной и указана в конфигурации. Для актуализации информации об устройстве ESDP, можно воспользоваться окном поиска (см. п. 2.2.2.6).

4.3 Обновление прошивок устройств с поддержкой протокола TLS

Обновление прошивок контроллеров Elsys-NG-1000, КСК Elsys-NG-Net II и совместимых с ними выполняется с помощью утилиты FtpUpdateUtility (см. Рисунок 86).

Файлы прошивок контроллеров доступа и КСК имеют расширение tge и загружаются через протокол FTP с использование сертификатов.

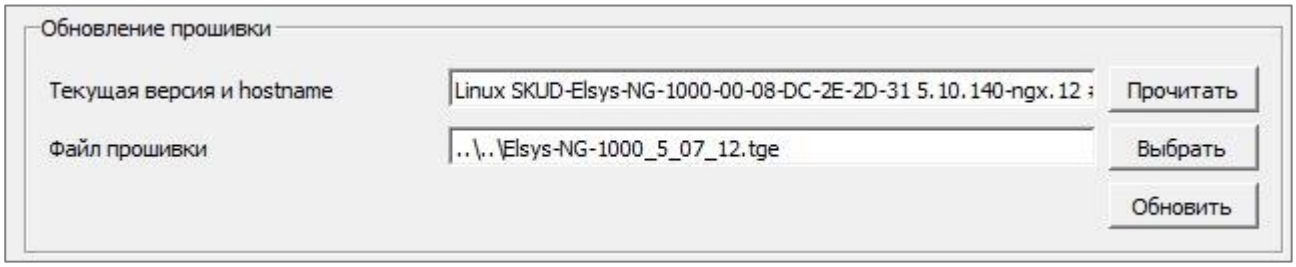

Рисунок 86. Обновление прошивки с помощью FtpUpdateUtility

Перед обновлением прошивки необходимо убедиться, что устанавливается связь с контроллером (см. 2.2.3.4).

Для обновления ПО контроллера необходимо выбрать файл прошивки с расширением tge, после чего нажать кнопку «Обновить». После завершения загрузки файла прошивки необходимо дождаться завершения обновления прошивки контроллера.

Внимание! Преждевременный сброс или выключение питания контроллера может привести к повреждению его прошивки.

5 Приложения

5.1 События устройств СКУД Elsys

5.1.1 События контроллеров

Таблица 14.

События контроллеров

Код события	Наименование события	Регистрация в протоколе	Регистрация номера карты	Использование во взаимодействиях	Дополнительные поля для взаимодействий
1	Выключение питания	+			
2	Включение питания	+			
3	Очистка конфигурации	+			
4	Разрушение БД контроллера	+			
5	Сброс программный	+		+	
6	Сброс аппаратный	+			
7	Срабатывание сторожевого таймера	+			
8	Взлом корпуса	+			
9	Восстановление зоны контроля взлома	+			
10	Потеря связи	+		+ (выполняется реакция на потерю связи с другими контроллерами)	Адрес контроллера (1 – 63, 0 – КСК, 64 – если необходимо обработать потерю связи с любым контроллером)

Код события	Наименование события	Регистрация в протоколе	Регистрация номера карты	Использование во взаимодействиях	Дополнительные поля для взаимодействий
11	Восстановление связи	+		+ (выполняется реакция на восстановление связи с другими контроллерами)	Адрес контроллера (1 – 63, 0 – КСК, 64 – если необходимо обработать восстановление связи с любым контроллером)
12	Авария первичного электропитания	+			
13	Восстановление первичного электропитания	+			
19	Сообщение от контроллера			+	1. Номер сообщения (1 - 64). 2. Адрес контроллера (1 – 63, 64 – любой контроллер).
20	Равенство счётчика значению			+	1. Номер счётчика (1 - 8). 2. Значение счётчика (0 – 63).
21	Равенство счётчика значению после увеличения			+	1. Номер счётчика (1 - 8). 2. Значение счётчика (0 – 63).
22	Равенство счётчика значению после уменьшения			+	1. Номер счётчика (1 - 8). 2. Значение счётчика (0 – 63).
23	Сброс антипассбэка	+			
37	Аккумулятор разряжен	+			
38	Аккумулятор в норме	+			
39	Восстановление буфера событий	+			
40	Частичное восстановление	+			

Код события	Наименование события	Регистрация в протоколе	Регистрация номера карты	Использование во взаимодействиях	Дополнительные поля для взаимодействий
	буфера событий				
41	Нет связи между Elsys-MB и Elsys-IP	+			
42	Восстановление связи между Elsys-MB и Elsys-IP	+			
43	Отсутствует модуль расширения памяти	+			
58	Отказ в доступе – нет полномочий	+	+		
59	Идентификация пользователя	+	+		
60	Постановка на охрану	+	+		
61	Снятие с охраны	+	+		
62	Идентификация пользователя WEB	+	+		
63	Потеря связи со считывателем	+			
64	Восстановление связи со считывателем	+			
65	Неисправность АДЛС1	+			
66	Неисправность АДЛС2	+			
67	Восстановление АДЛС1	+			
68	Восстановление АДЛС2	+			
69	Нарушение кольцевой топологии	+			
70	Восстановление кольцевой	+			

Код события	Наименование события	Регистрация в протоколе	Регистрация номера карты	Использование во взаимодействиях	Дополнительные поля для взаимодействий
	топологии				
71	Отключение WEB-клиента	+			
72	Подключение WEB-клиента	+			
73	Неверный PIN-код	+			
75	Обновление прошивки	+ (регистрирует конфигуратор)			
76	Замена сетевых параметров	+ (регистрирует конфигуратор)			
77	Ошибка при инициализации оборудования	+ (регистрирует конфигуратор)			
78	Инициализация оборудования	+ (регистрирует конфигуратор)			

5.1.2 События КСК

Таблица 15.

События КСК

Код события	**Наименование события**	**Регистрируется конфигуратором СКУД Elsys**
1	Выключение питания	
2	Включение питания	
3	Очистка конфигурации	
4	Разрушение БД контроллера	
5	Сброс программный	
6	Сброс аппаратный	
7	Срабатывание сторожевого таймера	
8	Взлом корпуса	
9	Восстановление зоны контроля взлома	
10	Потеря связи	
11	Восстановление связи	
33	Включение режима MULTIMASTER	
34	Включение режима MASTER-SLAVE	
35	Включение режима UDP	
36	Выключение режима UDP	
75	Обновление прошивки	+
76	Замена сетевых параметров	+
77	Ошибка при инициализации оборудования	+

Код события	Наименование события	Регистрируется конфигуратором СКУД Elsys
78	Инициализация оборудования	+
79	Ошибка при инициализации ОПС	+
80	Инициализация ОПС	+

5.1.3 События точек доступа

Таблица 16.

События точек доступа

Код события	Наименование события	Регистрация в протоколе	Регистрация номера карты	Использование во взаимодействиях	Дополнительные поля для взаимодействий
1	Штатный вход	+	+	+	
2	Вход под принуждением	+	+	+	
3	Штатный выход	+	+	+	
4	Выход под принуждением	+	+	+	
5	Дверь не заперта	+		+	
6	Взлом двери	+		+	
7	Удержание двери	+		+	
8	Закрытие двери	+		+	
9	Открытие двери	+		+	
10	КЗ дверного контакта	+		+	
11	Обрыв дверного контакта	+		+	
12	Нарушение зоны доступа при входе	+	+	+	

Код события	Наименование события	Регистрация в протоколе	Регистрация номера карты	Использование во взаимодействиях	Дополнительные поля для взаимодействий
13	Отказ в доступе на вход - нет прав	+	+	+	
14	Нарушение временной зоны при входе	+	+	+	
15	Неизвестная карта при входе	+	+	+	
16	Неизвестный PIN-код при входе	+	+	+	
17	Запрет входа - ограничение доступа	+	+	+	
18	Отказ в доступе на вход - блокировка	+	+	+	
19	Неверный PIN-код при входе	+	+	+	
20	Отказ в доступе - нет полномочий (вх. сч.)	+	+	+	
21	Ошибка ввода 1-й карты при входе	+	+	+	
22	Ошибка ввода 2-й карты при входе	+	+	+	
23	Любой отказ в доступе при входе			+	
24	Предъявлена первая карта при входе			+	
25	Предъявлена вторая карта при входе			+	
26	Предъявлена третья карта при входе			+	
27	Действие 1 (вх. сч.)	+	+	+	
28	Действие 2 (вх. сч.)	+	+	+	
29	Действие 3 (вх. сч.)	+	+	+	
30	Постановка на охрану вх. считывателем	+	+	+	
31	Снятие с охраны вх. считывателем	+	+	+	
34	Нарушение зоны доступа при выходе	+	+	+	
35	Отказ в доступе на выход - нет прав	+	+	+	
36	Нарушение временной зоны при выходе	+	+	+	
37	Неизвестная карта при выходе	+	+	+	

Код события	Наименование события	Регистрация в протоколе	Регистрация номера карты	Использование во взаимодействиях	Дополнительные поля для взаимодействий
38	Неизвестный PIN-код при выходе	+	+	+	
39	Запрет выхода - ограничение доступа	+	+	+	
40	Отказ в доступе на выход - блокировка	+	+	+	
41	Неверный PIN-код при выходе	+	+	+	
42	Отказ в доступе - нет полномочий (вых. сч.)	+	+	+	
43	Ошибка ввода 1-й карты при выходе	+	+	+	
44	Ошибка ввода 2-й карты при выходе	+	+	+	
45	Любой отказ в доступе при выходе			+	
46	Предъявлена первая карта при выходе			+	
47	Предъявлена вторая карта при выходе			+	
48	Предъявлена третья карта при выходе			+	
49	Действие 1 (вых. сч.)	+	+	+	
50	Действие 2 (вых. сч.)	+	+	+	
51	Действие 3 (вых. сч.)	+	+	+	
52	Постановка на охрану вых. считывателем	+	+	+	
53	Снятие с охраны вых. считывателем	+	+	+	
55	Фактический выход по кнопке	+			
56	Предоставление доступа на вход	+	+	+	
57	Предоставление доступа на выход	+	+	+	
58	Предост. доступа на вход под принуждением	+	+	+	
59	Предост. доступа на выход под принуждением	+	+	+	
60	Требуется подтверждение доступа при входе	+	+	+	
61	Требуется подтверждение доступа при выходе	+	+	+	

Код события	Наименование события	Регистрация в протоколе	Регистрация номера карты	Использование во взаимодействиях	Дополнительные поля для взаимодействий
62	Подтверждение доступа на вход оператором	+	+	+	
63	Подтверждение доступа на выход оператором	+	+	+	
64	Отказ в доступе на вход оператором	+	+	+	
65	Отказ в доступе на выход оператором	+	+	+	
66	Сброс режима подтверждения входного считывателя			+	
67	Сброс режима подтверждения выходного считывателя			+	
68	Блокировка	+		+	
69	Разблокировка	+		+	
70	Нормальный режим	+		+	
71	Блокировка выходной двери	+		+	
72	Разблокировка выходной двери	+		+	
73	Нормальный режим (выходная дверь)	+		+	
74	Неисправность дверного контакта	+		+	
75	Подтверждение доступа картой при входе	+		+	
76	Подтверждение доступа картой при выходе	+		+	
77	Ворота приоткрыты	+		+	
78	Открыть (команда)			+	
79	Закрыть (команда)			+	
80	Стоп (команда)			+	
81	Ввод пароля (входной считыватель)			+	Пароль (PIN-код)
82	Ввод пароля (выходной считыватель)			+	Пароль (PIN-код)

Код события	Наименование события	Регистрация в протоколе	Регистрация номера карты	Использование во взаимодействиях	Дополнительные поля для взаимодействий
83	Ввод пароля и предъявление карты (входной считыватель)	+	+	+	Пароль (PIN-код)
99	Ввод пароля и предъявление карты (выходной считыватель)	+	+	+	Пароль (PIN-код)
115	Штатное предъявление служебной карты (входной считыватель)			+	Номер карты
116	Штатное предъявление служебной карты (выходной считыватель)			+	Номер карты
117	Предъявление служебной карты (входной считыватель)			+	Номер карты
118	Предъявление служебной карты (выходной считыватель)			+	Номер карты
119	Вход с нарушением временной зоны	+	+		
120	Выход с нарушением временной зоны	+	+		
121	Вход с нарушением зоны доступа	+	+		
122	Выход с нарушением зоны доступа	+	+		
123	Предъявление карты с уровнем доступа (входной считыватель)			+	Номер уровня доступа (1 – 16382)
124	Предъявление карты с уровнем доступа (выходной считыватель)			+	Номер уровня доступа (1 – 16382)
130	На охране	+		+	
131	Снятие с охраны	+		+	
132	Невзятие			+	
133	Задержка взятия	+		+	

Код события	Наименование события	Регистрация в протоколе	Регистрация номера карты	Использование во взаимодействиях	Дополнительные поля для взаимодействий
134	Тревога входной зоны	+		+	
135	Тревога	+		+	
136	Штатный вход первого	+	+	+	
137	Штатный выход последнего	+	+	+	
138	Штатный вход первого с заданным УД	+	+	+	Номер уровня доступа (1 – 16382)
139	Штатный выход последнего с заданным УД	+	+	+	Номер уровня доступа (1 – 16382)
140	Изменение количества персонала			+	
141	Изменение количества персонала с заданным уровнем доступа			+	Номер уровня доступа (1 – 16382)
142	Удержание ключа/карты вх. сч.	+	+	+	
143	Удержание ключа/карты вых. сч.	+	+	+	
144	Отпускание ключа/карты вх. сч.			+	
145	Отпускание ключа/карты вых. сч.			+	
146	Вход не был совершён			+	
147	Выход не был совершён			+	
148	Идентификация пользователя (вх. сч.)	+	+	+	
149	Идентификация пользователя (вых. сч.)	+	+	+	
152	Восст. связи со считывателем (вх. сч.)	+			
153	Восст. связи со считывателем (вых. сч.)	+			
154	Потеря связи со считывателем (вх. сч.)	+			
155	Потеря связи со считывателем (вых. сч.)	+			

5.1.4 События считывателей

Таблица 17.

События считывателей

Код события	Наименование события	Регистрация номера карты	Используется только в охранных контроллерах	Регистрируется конфигуратором Elsys
20	Отказ в доступе – нет полномочий	+	+	
30	Постановка на охрану	+	+	
31	Снятие с охраны	+	+	
75	Обновление прошивки			+
77	Ошибка при инициализации оборудования			+
78	Инициализация оборудования			+
81	Загрузка профиля безопасности			
82	Ошибка загрузки профиля безопасности			
148	Идентификация пользователя	+	+	
150	Идентификация пользователя WEB	+	+	
152	Восстановление связи со считывателем		+	
154	Потеря связи со считывателем		+	
155	Восстановление связи с камерой распознавания			
156	Потеря связи с камерой распознавания			
157	Восстановление питания			
158	Авария питания			
159	Восстановление зоны контроля взлома			

Код события	Наименование события	Регистрация номера карты	Используется только в охранных контроллерах	Регистрируется конфигуратором Elsys
160	Взлом корпуса			

5.1.5 События входов

Таблица 18.

События входов

Код события	Наименование события	Регистрация в протоколе	Регистрация номера карты	Использование во взаимодействиях	Дополнительные поля для взаимодействий
1	Обрыв	+			
2	Короткое замыкание	+			
3	Норма (готов к взятию на охрану)	+		+	
4	Неготовность	+		+	
5	На охране	+		+	
6	Тревога	+		+	
7	Удержание	+		+	
8	Невзятие	+		+	
9	Снятие с охраны	+		+	
10	Неисправность			+	
11	Задержка взятия	+		+	
12	Задержка взятия - неготовность	+		+	
13	Задержка тревоги	+		+	
14	Взлом корпуса	+			

Код события	Наименование события	Регистрация в протоколе	Регистрация номера карты	Использование во взаимодействиях	Дополнительные поля для взаимодействий
15	Восстановление корпуса	+			
16	Потеря связи	+			
17	Восстановление связи	+			
18	Ошибка конфигурации	+			

5.1.6 События выходов

Таблица 19.

События выходов

Код события	Наименование события	Регистрация в протоколе	Регистрация номера карты	Использование во взаимодействиях	Дополнительные поля для взаимодействий
1	Включение	+		+	
2	Выключение	+		+	
3	Окончание работы по формуле	+		+	
4	Включение работы по формуле	+			
5	Взлом корпуса	+			
6	Восстановление корпуса	+			
7	Потеря связи	+			
8	Восстановление связи	+			
9	Ошибка конфигурации	+			

5.1.7 События разделов и групп разделов

Таблица 20.

События разделов и групп разделов

Код события	Наименование события	Регистрация в протоколе	Регистрация номера карты	Использование во взаимодействиях	Дополнительные поля для взаимодействий
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	+			
9	Запрос на взятие	+	+		
10	Запрос на снятие	+	+		
11	Неисправность при взятии	+	+		
12	Неисправность при снятии	+	+		
13	Недоступно для управления	+	+		
14	Нет полномочий для взятия на охрану	+	+		
15	Нет полномочий для снятия с охраны	+	+		
16	Взятие на охрану пользователем	+	+		
17	Снятие с охраны пользователем	+	+		
18	Невзятие на охрану пользователем	+	+		

5.2 Команды управления устройствами СКУД Elsys

5.2.1 Команды управления дверями

Таблица 21.

Команды управления дверями

Код команды	Наименование команды	Управление через ПО	Участие во взаимодействиях	Дополнительные параметры для взаимодействий
0	Открыть	+	+	
1	Заблокировать	+	+	
2	Нормальный режим	+	+	
3	Разблокировать	+	+	

5.2.2 Команды управления турникетами

Таблица 22.

Команды управления турникетами

Код команды	Наименование команды	Управление через ПО	Участие во взаимодействиях	Дополнительные параметры для взаимодействий
0	Открыть на вход	+	+	
1	Заблокировать на вход	+	+	
2	Нормальный режим на вход	+	+	
3	Разблокировать на вход	+	+	
4	Открыть на выход	+	+	
5	Заблокировать на выход	+	+	
6	Нормальный режим на выход	+	+	
7	Разблокировать на выход	+	+	

Код команды	Наименование команды	Управление через ПО	Участие во взаимодействиях	Дополнительные параметры для взаимодействий
8	Заблокировать на вход и на выход	+		
9	Нормальный режим на вход и на выход	+		
10	Разблокировать на вход и на выход	+		

5.2.3 Команды управления воротами

Таблица 23.

Команды управления воротами

Код команды	Наименование команды	Управление через ПО	Участие во взаимодействиях	Дополнительные параметры для взаимодействий
0	Открыть	+	+	
1	Заблокировать	+	+	
2	Нормальный режим	+	+	
4	Закрыть	+	+	
5	Остановить	+	+	

5.2.4 Команды управления контроллерами

Таблица 24.

Команды управления контроллером, передаваемые через управляющее ПО

Код команды	Наименование команды	Дополнительные параметры
0	Сброс	
1	Сброс глобального контроля последовательности прохода	

Код команды	Наименование команды	Дополнительные параметры
2	Очистка конфигурации	
4	Сброс всех устройств, обслуживаемых контроллером, в исходное состояние	
5	Сброс счётчика персонала	
102	Восстановление протокола событий	Дата и время, начиная с которых необходимо восстановить протокол событий

Таблица 25.

Команды с участием контроллера, используемые во взаимодействиях

Код команды	Наименование команды	Дополнительные параметры для взаимодействий	
		Параметр 1	Параметр 2
1	Сформировать сообщение контроллерам	Номер сообщения (1 – 64)	Адрес контроллера (1 – 63; 0 – сообщение передаётся всем контроллерам)
2	Инкремент счётчика	Номер счётчика (1 – 8)	
3	Декремент счётчика	Номер счётчика (1 – 8)	
4	Установить значение счётчика	Номер счётчика (1 – 8)	Значение счётчика (0 – 63)
5	Сброс счётчика персонала		
6	Сброс счётчика персонала для УД	Номер УД (1 – 16382)	

5.2.5 Команды управления считывателями

Таблица 26.

Команды управления считывателями

Код команды	**Наименование команды**	**Управление через ПО**	**Участие во взаимодействиях**	**Дополнительные параметры для взаимодействий**
0	Заблокировать	+	+	Время блокировки. Если значение параметра 0, выполняется блокировка считывателя. иначе выполняется блокировка на заданное время (1 – 63 с), по истечении которого считыватель возвращается в нормальный режим
1	Нормальный режим	+	+	Время включения нормального режима. Если значение параметра 0, считыватель переводится в нормальный режим, иначе нормальный режим включается на заданное время (1 – 63 с), по истечении которого считыватель возвращается в режим блокировки.
2	Ограничить доступ	+	+	
3	Снять ограничения доступа	+	+	

5.2.6 Команды управления входами

Таблица 27.

Команды управления входами

Код команды	Наименование команды	Управление через ПО	Участие во взаимодействиях	Дополнительные параметры для взаимодействий
0	Снять с охраны	+	+	Время задержки постановки на охрану в секундах (0 – 127).
1	Поставить на охрану	+	+	Время шунтирования входа в секундах (0 – 127). Если параметр равен 0, выполняется снятие с охраны, иначе – выполняется шунтирование входа, т. е. снятие с охраны на заданное время.

5.2.7 Команды управления выходами

Таблица 28.

Команды управления выходами

Код команды	Наименование команды	Управление через ПО	Участие во взаимодействиях	Дополнительные параметры для взаимодействий
0	Выключить	+	+	
1	Включить по формуле	+ (при управлении используется формула, описывающая импульс длительностью 1 с)	+	Номер формулы управления выходом
2	Включить	+	+	
3	Инвертировать состояние выхода	–	+	

5.2.8 Команды управления разделами

Таблица 29.

Команды управления разделами

Код команды	Наименование команды	Управление через ПО	Участие во взаимодействиях	Дополнительные параметры для взаимодействий
0	Снять с охраны	+	+	
1	Поставить на охрану	+	+	