Бастион-3 – Elsys. Руководство администратора

Версия 2024.2

(08.04.2024)

Самара, 2024

Оглавление

1 Общие сведения

1.1 Назначение и область применения

Драйвер «Бастион-3 – Elsys» предназначен для мониторинга и управления системы контроля и управления доступом (СКУД) Elsys (ООО «ЕС-пром», Группа компаний «ТвинПро»).

Драйвер обеспечивает поддержку всей номенклатуры оборудования СКУД Elsys - контроллеров доступа Elsys-MB вариантов исполнения Pro, Standard, Light, Pro4, SM, контроллеров Elsys-NG-200, Elsys-NG-400, Elsys-NG-800 и Elsys-NG-1000, контроллеров линейки ЛКД-КС-2000, модулей Elsys-IO/MB, коммуникационных сетевых контроллеров Elsys-MB-Net и Elsys-MB-Net II (далее – КСК), а также приборов охранной подсистемы Elsys-MB-AC, Elsys-RM16, Elsys-CP1, Elsys-AC2, Elsys-CDP и Elsys-CP2.

1.2 Структура СКУД Elsys

Обобщённая структурная схема СКУД Elsys приведена на Рис. 1.

Контроллеры могут быть объединены в сеть по двухпроводному интерфейсу RS-485 (до 63 контроллеров в одной линии связи) и подключены к коммуникационному сетевому контроллеру Elsys-MB-Net или Elsys-MB-Net II. Кроме того, контроллеры Elsys-MB старших моделей (Pro, Standard, Light, Pro4) могут быть оснащены интерфейсным Ethernet-модулем Elsys-IP (в этом случае они обозначаются как Elsys-MB-IP) и подключены к ПК через локальную вычислительную сеть Ethernet. А модули охранной подсистемы Elsys-RM16, Elsys-AC2, Elsys-CP2 уже имеют в своем составе Ethernet-модули и могут быть подключены в вычислительную сеть непосредственно.

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

Взаимодействие оборудования с драйвером «Бастион-3 – Elsys» осуществляется через «Сервис программного SDK Elsys» (далее — Сервис интеграции), работающий на одном из компьютеров системы (например на «Сервере оборудования», совместно с экземпляром драйвера «Бастион-3 – Elsys»).

Каждый экземпляр драйвера «Бастион-3 – Elsys» поддерживает до 255 КСК и до 254 сетевых групп.

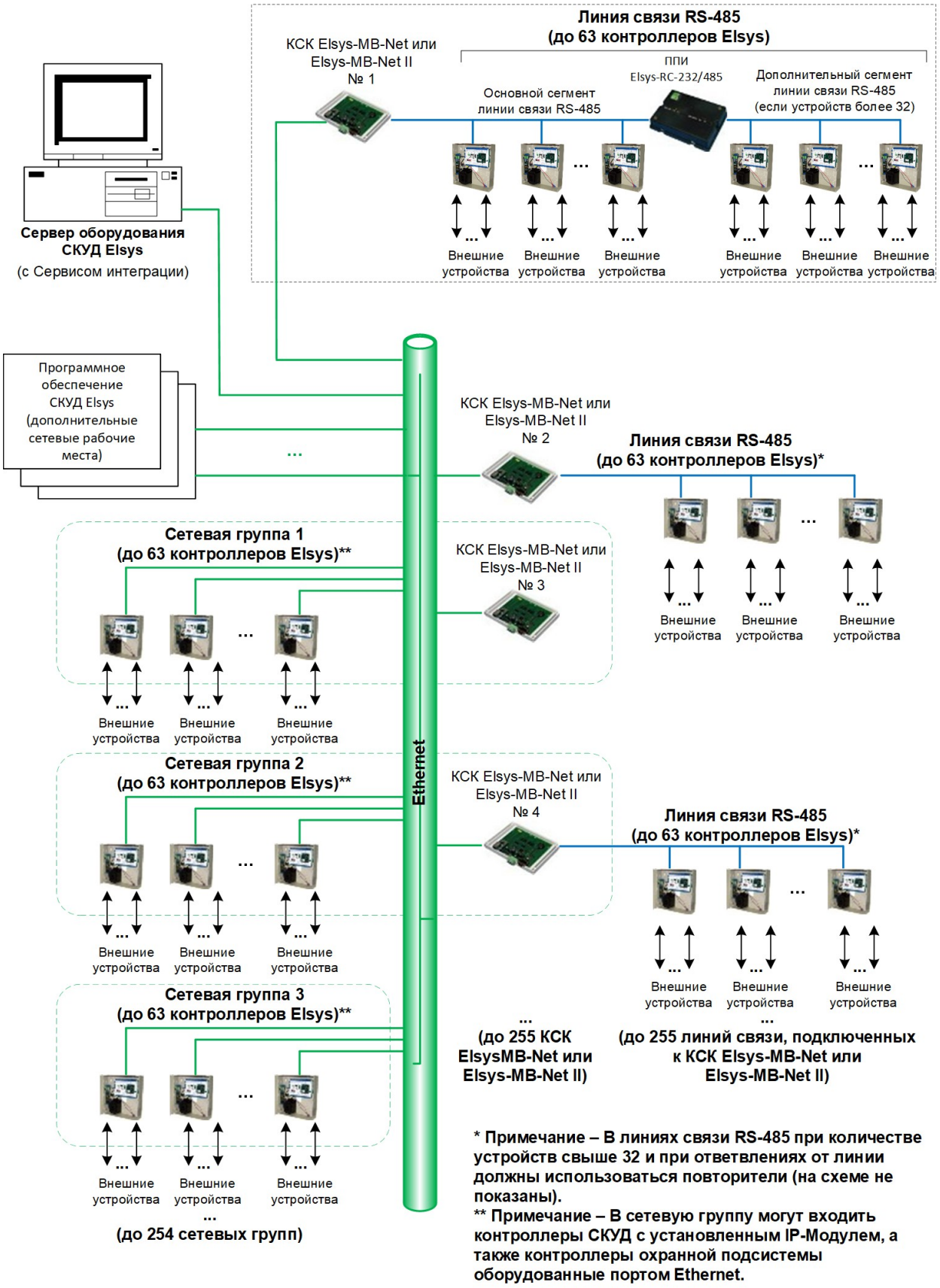


Рис. 1. Структурная схема СКУД Elsys

2 Условия применения

2.1 Требования к совместимости

Драйвер «Бастион-3 – Elsys» функционирует в составе ПК «Бастион-3», требования к программному обеспечению полностью соответствуют изложенным в документе «*Бастион-3. Руководство администратора».*
Драйвер совместим с ПК «Бастион-3» версии 2023.1 и выше.

2.2 Лицензирование

В драйвере «Бастион-3 – Elsys» применяются лицензионные ограничения на общее количество адресуемых контроллеров в системе.
Драйвер не обеспечивает работу с приборами свыше лицензионных ограничений. В случае недостатка лицензий драйвер формирует сообщение «Нет лицензий», в котором указывается количество требуемых и полученных лицензий, и прекращает свою работу.

2.3 Требования к подготовке пользователя

Перед началом настройки СКУД Elsys необходимо ознакомиться с документами «Руководство системного администратора», «Рекомендации по комплектации и проектированию СКУД Elsys», «Руководство по эксплуатации СКУД Elsys», а также с руководствами по эксплуатации на всё используемое оборудование.

3 Настройка драйвера

3.1 Порядок настройки

Перед добавлением драйвера «Бастион-3 – Elsys» и настройкой его работы в составе ПК «Бастион-3» необходимо выполнить следующие шаги:

- произвести первоначальную настройку оборудования: задать адреса устройств на линии связи, IP-адреса, маску подсети и адрес шлюза для устройств, работающих по интерфейсу Ethernet в соответствии с инструкцией по эксплуатации на настраиваемое оборудование;

- установить, настроить и запустить Сервис интеграции («Сервис программного SDK Elsys») ElsysAppService (см. документ «ElsysAppService. Руководство администратора»);

- установить «Конфигуратор СКУД Elsys» (далее Конфигуратор оборудования);

- если не предполагается хранить конфигурации оборудования в базе данных ПК «Бастион-3» можно произвести конфигурирование всех устройств, работающих в составе СКУД (см. документ «Конфигуратор СКУД Elsys. Руководство пользователя») запустив автономно Конфигуратор оборудования;

- убедиться в наличии лицензий для работы драйвера «Бастион-3 – Elsys»;

- добавить драйвер (см. п. 3.2) и настроить подключение к Сервису интеграции.

- если предполагается хранить конфигурации оборудования в базе данных АПК «Бастион-3», необходимо настроить в Менеджере конфигураций оборудования вариант хранения конфигурации, и запустив от туда конфигуратор произвести конфигурирование всех устройств, работающих в составе СКУД (см. документ «Конфигуратор СКУД Elsys. Руководство пользователя»)

> **Внимание!** В случае хранения конфигурации оборудования в базе данных АПК «Бастион-3» запускать конфигуратор необходимо только из панели управления АПК «Бастион-3»!

- после настройки конфигурации оборудования необходимо произвести её импорт из сервиса интеграции.

3.2 Добавление драйвера

Добавление драйвера в ПК «Бастион-3» описано в документе «Бастион-3. Руководство администратора» в разделе «Конфигурация драйверов».

3.3 Меню драйвера

После добавления драйвера в разделе **«Драйверы»** появится лента управления **«Драйвер СКУД Elsys»** (Рис. 2).

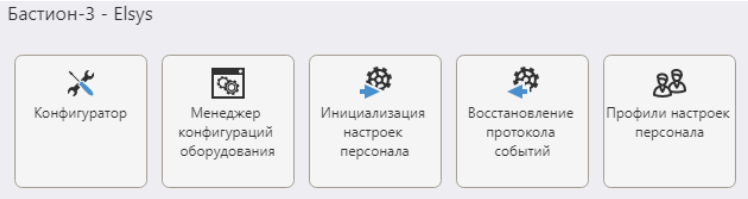


Рис. 2. Лента управления драйвером «Бастион-3 – Elsys»

Кнопка **«Конфигуратор»** вызывает «Общий конфигуратор драйверов», предназначенный для настройки подключения к Сервису интеграции, а также задания часовых поясов для оборудования.

Кнопка **«Менеджер конфигураций оборудования»** вызывает панель для запуска Конфигуратора оборудования и управления конфигурациями оборудования.

Кнопка **«Инициализация настроек персонала»** позволяет проверить состояние контроллеров (наличие связи, число карт, уровней доступа и т. д.) и записать в контроллеры настройки областей контроля, карты и уровни доступа, настройки управления охранной сигнализации. (более подробно см. п. 3.8).

Кнопка **«Восстановление протокола событий»** позволяет повторно получить из контроллеров хранящиеся в них события за указанный интервал времени.

Кнопка **«Профили настроек персонала»** позволяет настроить дополнительные полномочия пользователя, обеспечивающие организацию специфических условий доступа (более подробно см. п. 3.8.1).

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

3.4 Настройка подключения к сервису интеграции

При первом запуске драйвера в окне настройки Сервиса интеграции следует указать параметры подключения, заданные при конфигурировании оборудования (Рис. 3) и сохранить настройку.

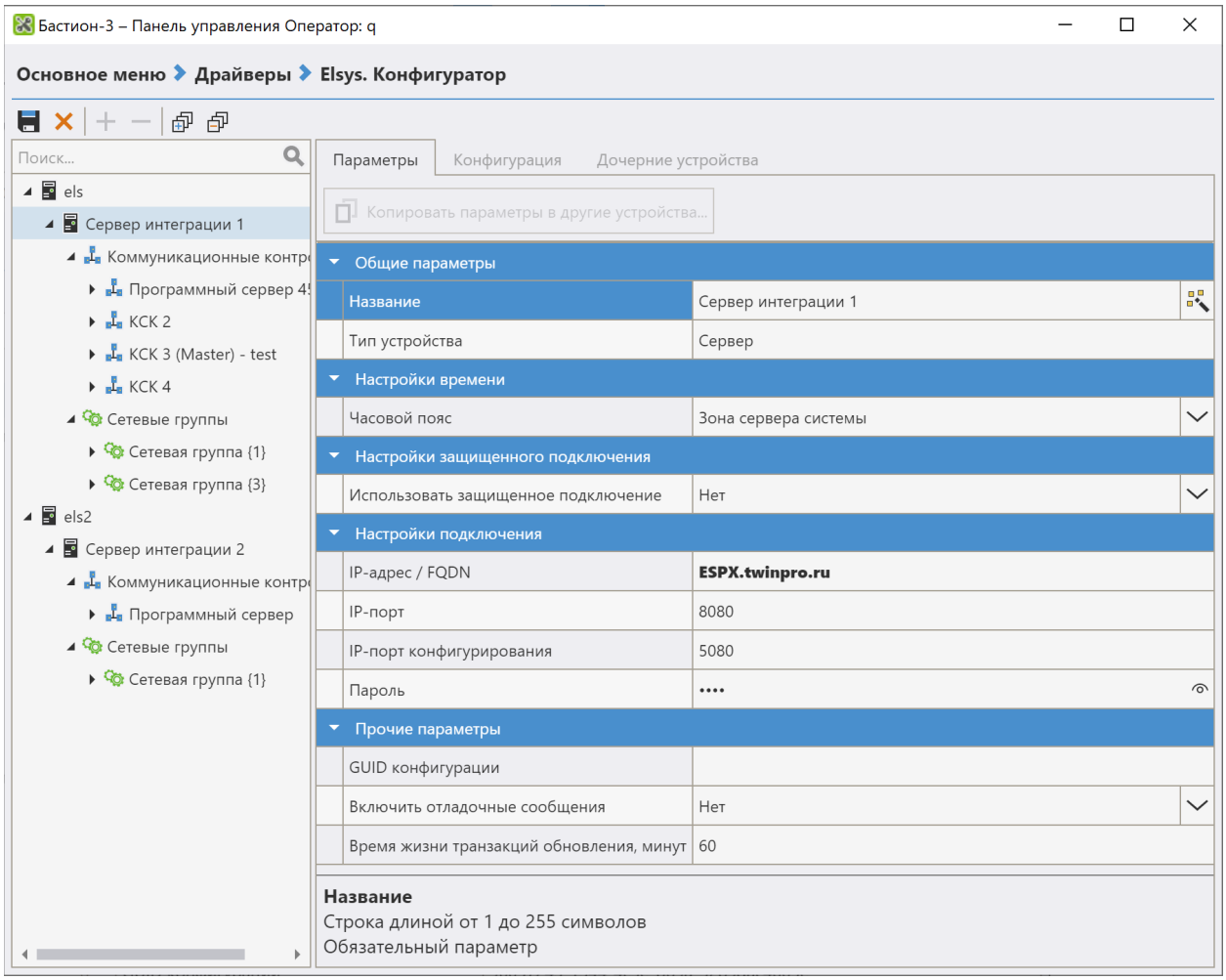


Рис. 3. Окно настройки драйвера «Бастион-3 – Elsys»

При необходимости использования дополнительного SSL-шифрования при обмене информации между драйвером и программным сервисом интеграции требуется настроить защитное подключение. Для этого необходимо выбрать «Да» в пункте «Использовать защищенного подключения» и указать требуемые параметры (Рис. 4)

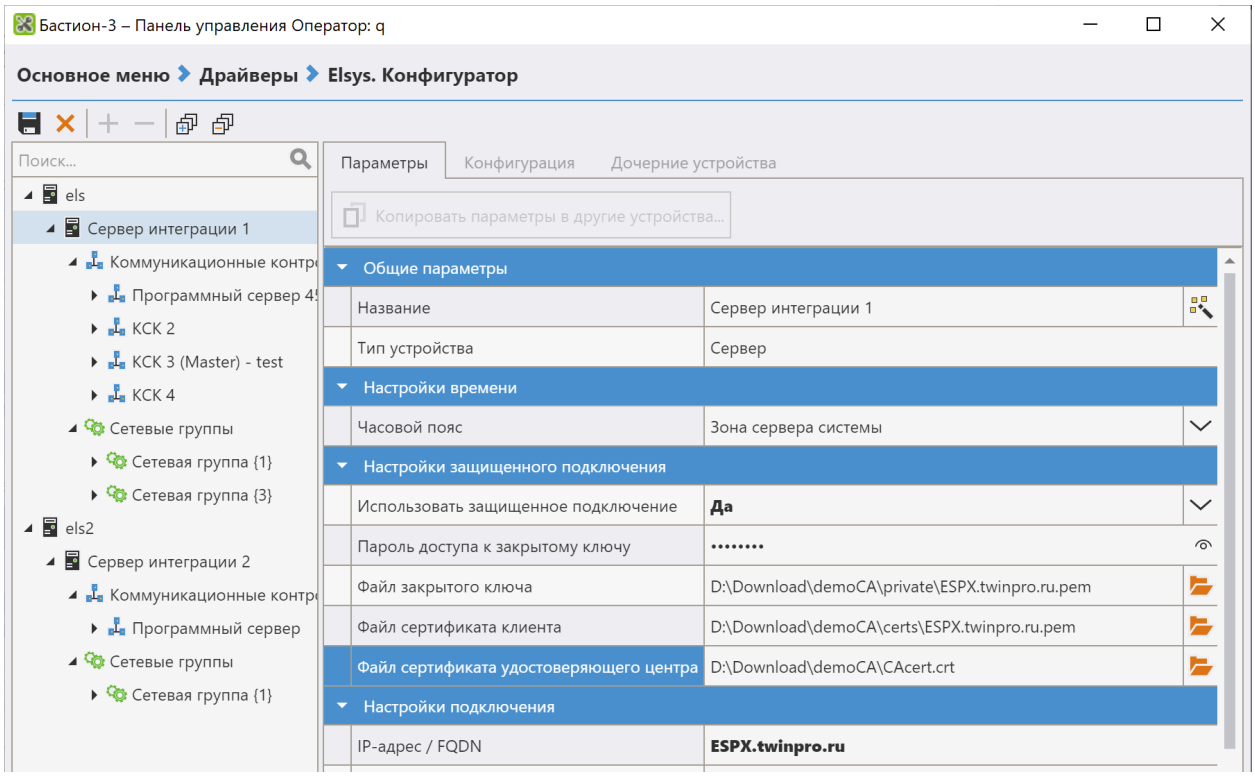


Рис. 4. Окно настройки защищенного подключения

После сохранения настроек драйвер автоматически перезапустится.

3.5 Конфигурирование оборудования и управление конфигурациями

Для настройки оборудования используется отдельное ПО «Конфигуратора СКУД Elsys» (далее — Конфигуратор оборудования) описание работы с которым приведено в документе «Конфигуратор СКУД Elsys. Руководство пользователя».

Запуск Конфигуратора оборудования осуществляется либо автономно — пользователем из операционной системы, либо через раздел «Менеджер конфигураций оборудования» «Панели управления». В последнем случае доступно сохранение конфигураций и управление ими в ПК «Бастион-3» (по умолчанию отключено — хранение конфигурации оборудования осуществляется в Сервисе интеграции).

Если предполагается хранение конфигурации оборудования не в Сервисе интеграции, а в базе данных ПК «Бастион-3», то необходимо **всегда** запускать Конфигуратор оборудования Elsys через раздел «Менеджер конфигураций оборудования» «Панели управления».

В процессе работы при необходимости возможно изменить вариант хранения конфигураций, а переносить конфигурации из Сервиса интеграции в базу ПК «Бастион-3» и обратно возможно через процедуры импорта/экспорта.

3.5.1 Управление конфигурациями оборудования

Управление конфигурациями оборудования доступно на панели «Менеджер конфигураций оборудования» в «Панели управления» ПК «Бастион-3» (Рис. 4)

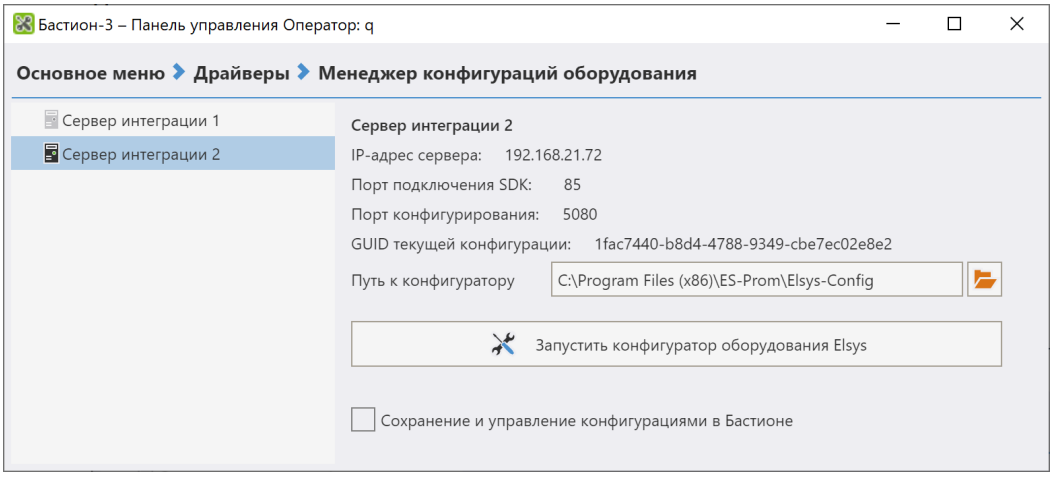


Рис. 5. Окно управления конфигурациями оборудования

В левой части окна располагается список добавленных Сервисов интеграции, при этом если Сервис на связи, его иконка будет яркой.

В правой части окна отображаются свойства выбранного Сервиса интеграции, а также общие настройки, необходимые для запуска Конфигуратора оборудования.

«Путь к конфигуратору» – указывает расположение исполняемого файла Конфигуратора оборудования на локальном рабочем месте.

Если выбранный Сервис интеграции работает с использованием защищенного подключения, то становятся доступны соответствующие настрой для клиента (Рис. 4).

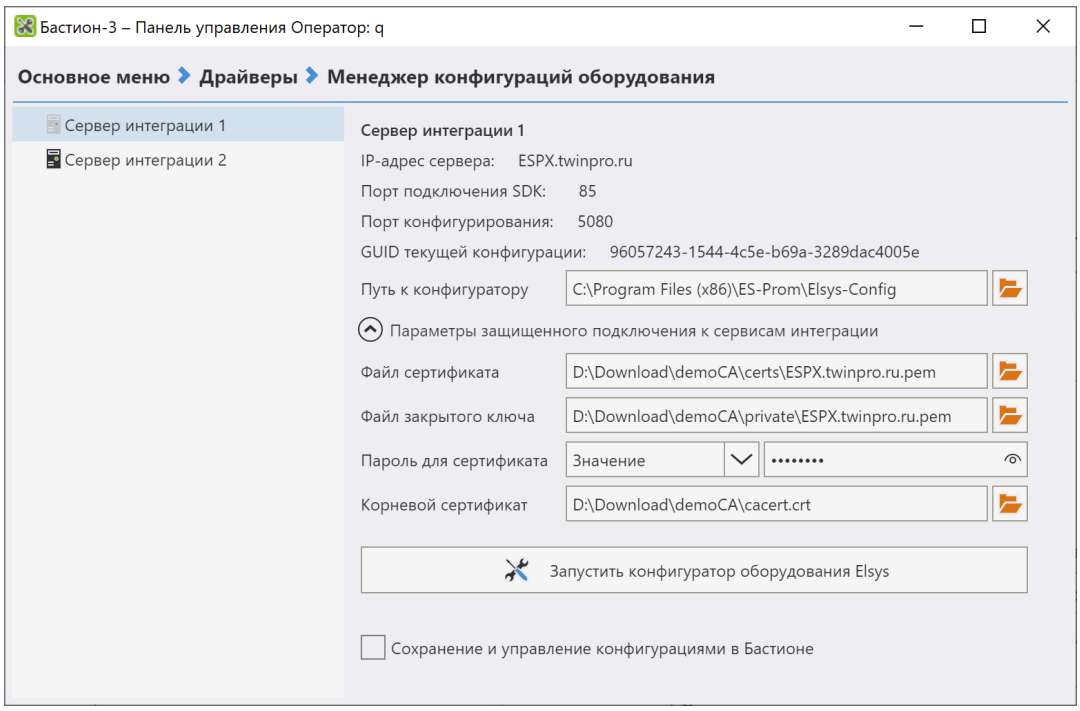


Рис. 6. Параметры защищенного подключения к сервисам интеграции

Если установлен флаг «Сохранение и управление конфигурациями в Бастионе», то станет доступен список сохраненных в базе данных ПК «Бастион-3» конфигураций оборудования (Рис. 4). Активная конфигурация (инициализированная в Сервисе интеграции и синхронизированная с драйвером «Бастион-3 — Elsys», будет выделена жирным шрифтом.

Новую конфигурацию можно импортировать из файла, нажав кнопку «Импорт из файла». Также все сохранения конфигурации, сделанные в Конфигураторе оборудования фиксируются в базе данных ПК «Бастион-3».

В списке можно выделить требуемую конфигурацию и выполнить следующие действия:

«Экспорт в файл» - для экспорта выбранной конфигурации оборудования из базы данных ПК «Бастион-3», например для дальнейшей работы в автономно запущенном Конфигураторе оборудования.

«Удалить» - для удаления выбранной конфигурации оборудования из базы данных ПК «Бастион-3».

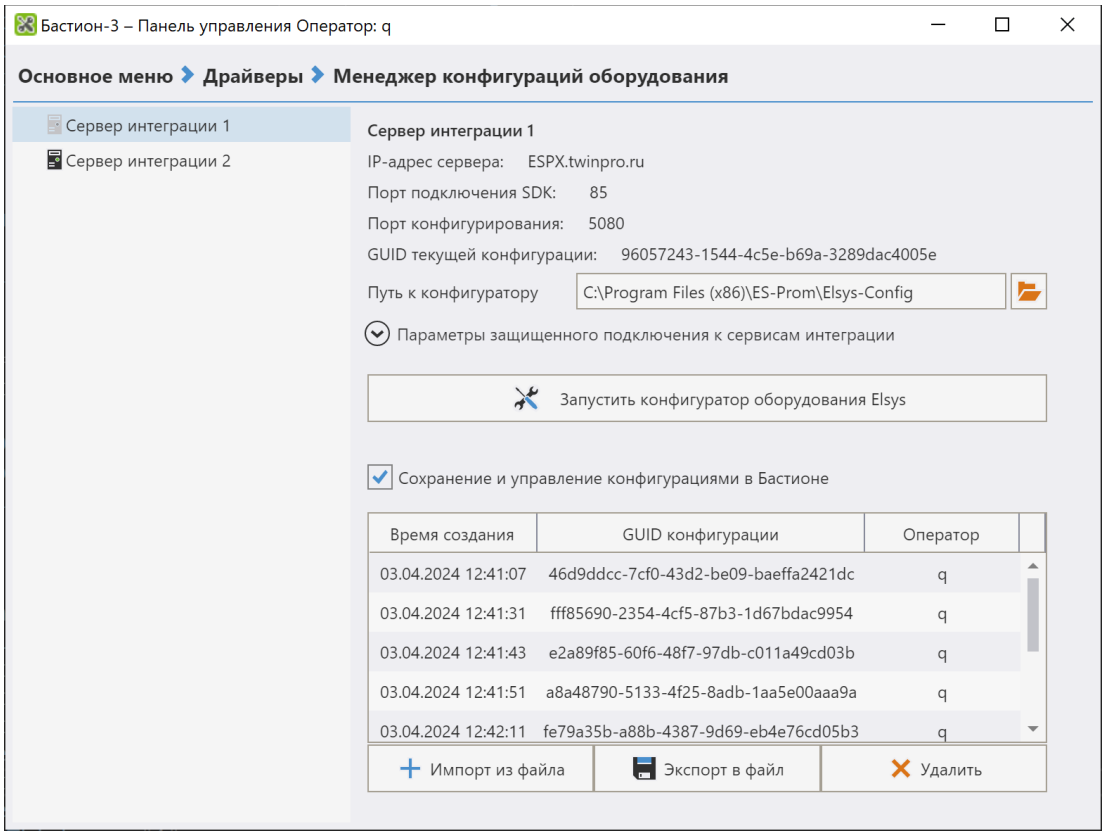


Рис. 7. Управление конфигурациями оборудования

Запуск Конфигруатора оборудования осуществляется нажатием соответскующей кнопки. При этом если используется Сохранение и управление конфигурациями в Бастионе, **в Конфигуратор оборудования передается последняя из сохраненных конфигурация**.

3.6 Импорт конфигураций оборудования в драйвер

После изменения конфигурации оборудования и инициализации Сервиса интеграции необходимо получить или обновить дерево устройств драйвера. Для этого следует нажать кнопку **«Конфигуратор»** в ленте управления драйвером (Рис. 2).

На вкладке «Конфигурация» необходимо импортировать текущую конфигурацию из Сервиса интеграции (Рис. 8).

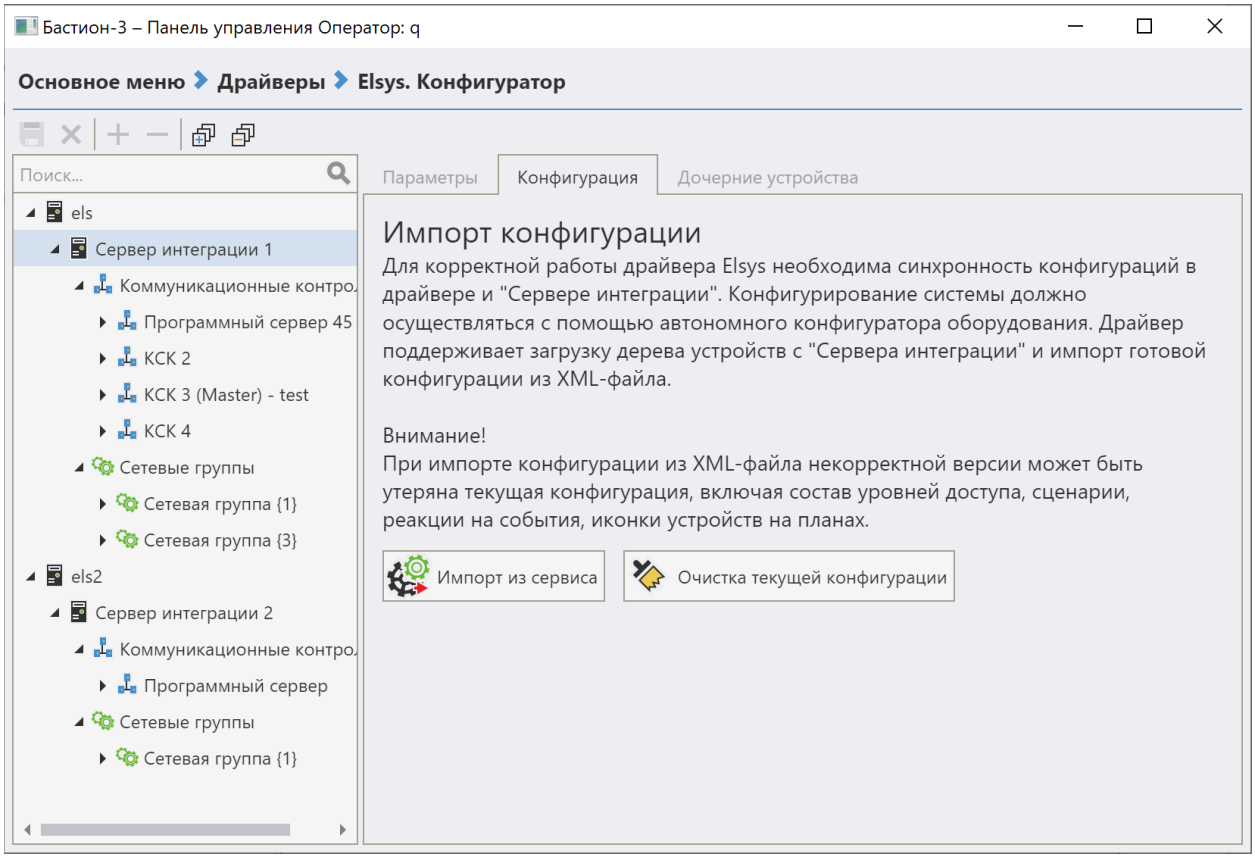


Рис. 8. Окно импорта конфигурации

Если были введены корректные настройки подключения и сервис интеграции доступен, то конфигуратор драйвера прочитает новое дерево устройств из Сервиса интеграции и при наличии в ней изменений предложит заменить названия из новой конфигурации (Рис. 9).

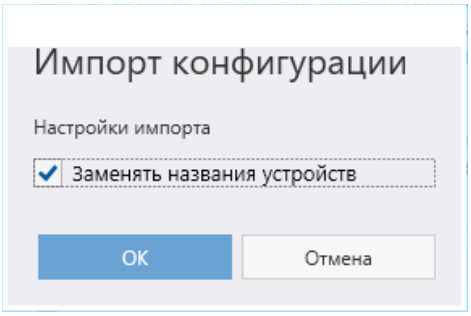
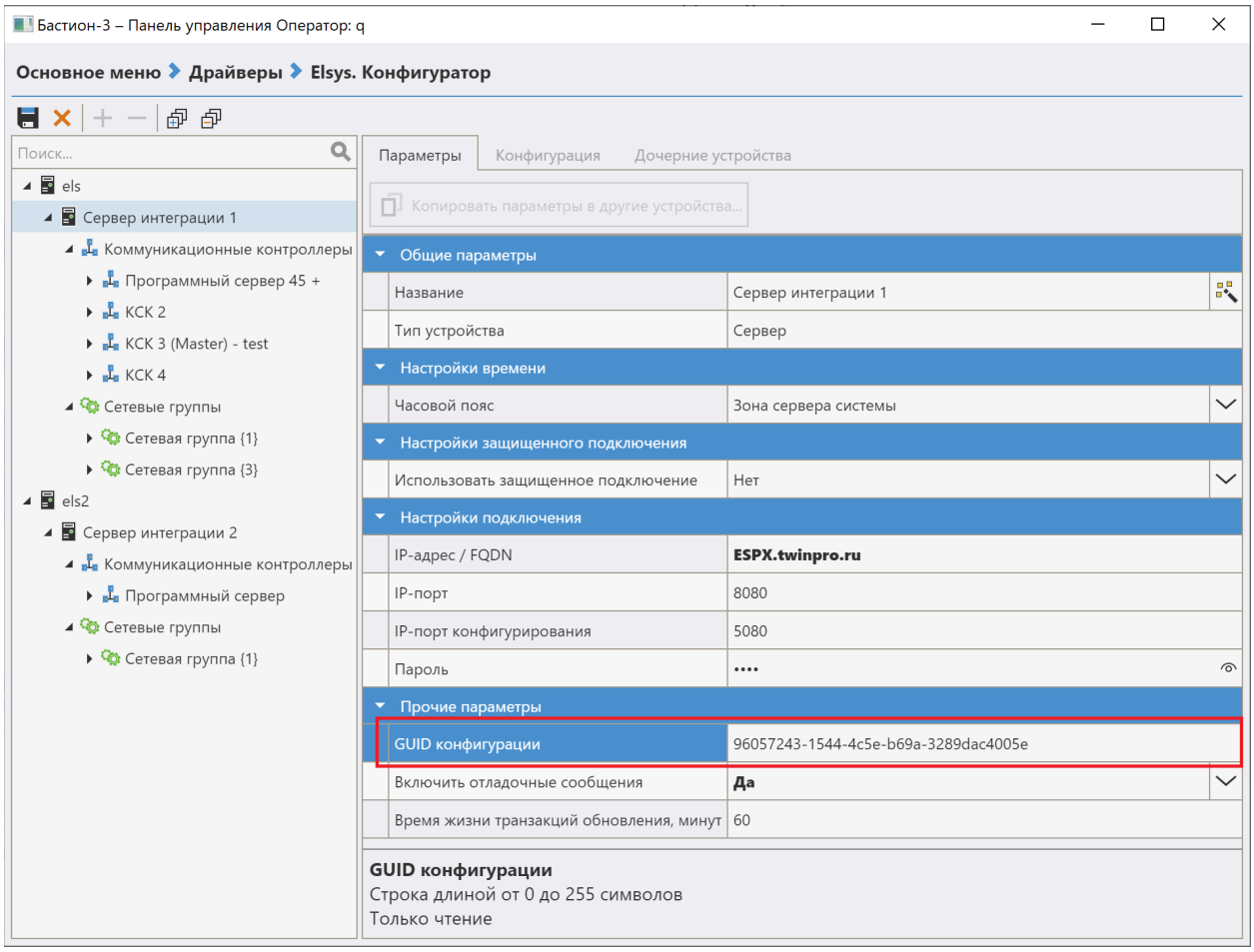


Рис. 9. Запрос настроек импорта конфигурации

После успешного импорта в окне конфигуратора отобразится полученное дерево устройств, а в настройках сервиса интеграции отобразится текущий GUID (идентификатор) конфигурации (Рис. 10).

Рис. 10. Дерево устройств в общем конфигураторе



При необходимости можно изменить названия устройств, заданные при конфигурировании оборудования (Рис. 11).

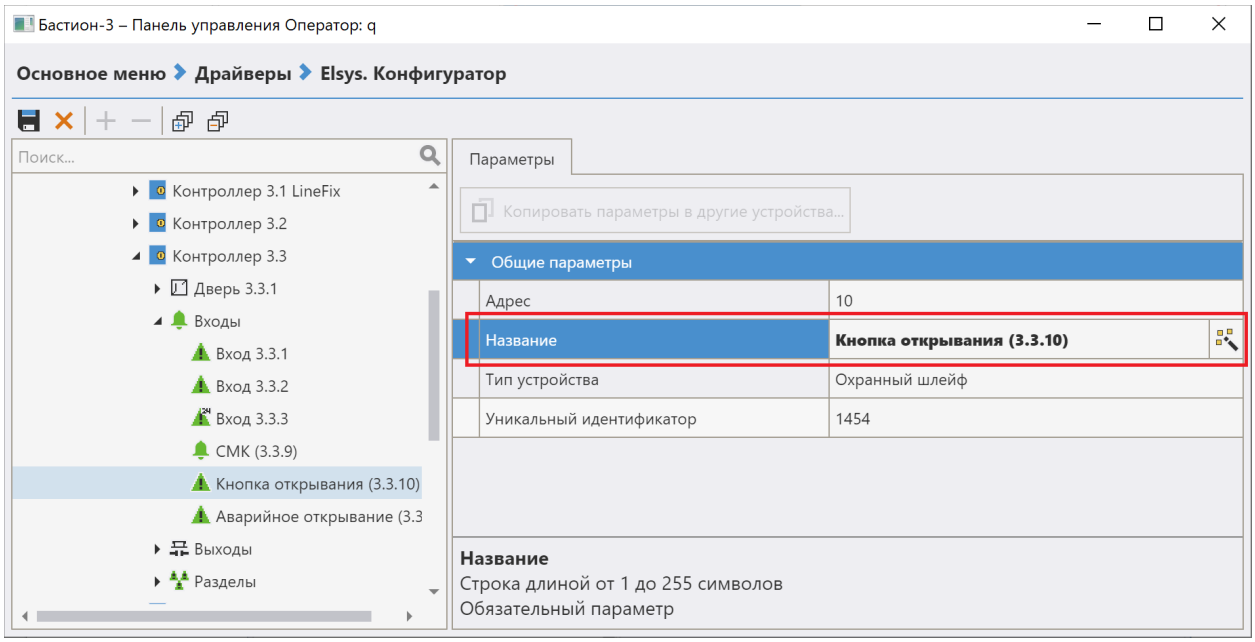


Рис. 11. Пометка доступных для редактирования полей

По завершении работы следует сохранить настройки.

Более подробно работа с «Общим конфигуратором драйверов» описана в документе «Бастион-3. Руководство администратора».

3.7 Настройка глобального контроля последовательности прохода

3.7.1 Описание работы глобального контроля последовательности прохода

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

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

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

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

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

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

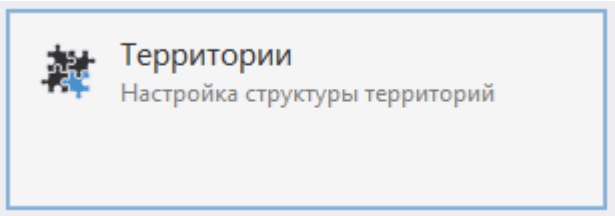
Глобальный antipassback функционирует в пределах единого информационного пространства, в котором возможен обмен информацией между контроллерами. Единое информационное пространство может быть создано:

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

Каждый КСК Elsys-MB-Net может обслуживать одну линию связи RS-485 (до 63 УУ Elsys-MB) и/или одну сетевую группу (до 63 УУ Elsys-MB-IP). Суммарное число линий связи и сетевых групп в одной системе может достигать 254.

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

Для работы глобального контроля последовательности прохода, а также для управления пропусками используются объекты «Территория», которые добавляются и настраиваются в разделе «Структура объекта» - «Территории»



Вся территория предприятия, обслуживаемая СКУД, представляет или несколько вложенных объектов «Территория». По умолчанию существуют две «Территории» **«На территории»** и **«Вне территории»** (последняя не видна для пользователя, а доступна только при конфигурировании). Для более сложных конфигураций могут быть созданы дополнительные вложенные «Территории».

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

территории в качестве входной и выходной – в этом случае считается, что точка доступа находится внутри «Территории».

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

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

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

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

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

При использовании глобального контроля последовательности прохода следует учитывать, что в перечисленных ниже случаях выполняется сброс состояния пользователей для «Территорий» в контролерах (для карт доступа устанавливается состояние *"Разрешён вход и выход"*):

- после выполнения из окна инициализации команды «Сброс антипассбэка», адресованной конкретному контроллеру;
- после сброса или выключения питания контроллера;

- после потерь связи с другими контроллерами (если выключена опция «Не отслеживать исправность областей контроля»);
- после инициализации оборудования, карт доступа, областей контроля;
- после редактирования «Территорий» (т. к. вслед за этим следует автоматическая доставка изменений областей контроля);
- после изменения настроек АПБ в оборудовании (в этом случае после сохранения настроек происходит перезапуск драйвера и требуется обновление конфигурации и инициализация);
- после редактирования свойств пропуска – только для конкретного пропуска;
- в полночь (если включена настройка «Сброс в полночь»);
- по функции «временной antipassback» – для конкретных пропусков отдельно.

Для работы глобального контроля последовательности прохода необходимо:

- назначить адреса контроллерам по порядку, без пропусков (в каждой линии связи RS-485 адреса должны начинаться с «1», т. к. наличие пропусков адресах, нумерация не с «1», исключенные из опроса контроллеры, приводят к снижению скорости работы системы в режиме Multimaster);
- обновить прошивки контроллеров (использование контроллеров Elsys-MB с версией прошивки ниже 2.63 и Elsys-SM версии ниже 2.20 приведёт к снижению быстродействия системы);
- настроить единое информационное пространство, включив antipassback и обмен данными между контроллерами (п. 3.7.2);
- настроить области контроля (п. 3.7.3);
- проверить корректность настройки оборудования для работы глобального контроля последовательности прохода с учетом настроек областей контроля.

3.7.2 Настройка системы для работы глобального контроля последовательности прохода

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

1) установлены взаимосвязи КСК Elsys-MB-Net и сетевых групп (если они используются и участвуют в едином информационном пространстве);
2) режим обмена в линии связи RS-485 - MULTIMASTER;
3) обмен информацией всех контроллеров в сетевой группе между собой - включен;

4) обмен информацией КСК Elsys-MB-Net между собой - включен;

5) глобальный контроль последовательности прохода в каждой линии связи и сетевой группе – включен.

Для конфигурирования оборудования для работы глобального контроля последовательности прохода используется Автономный конфигуратор. Работа с «Автономным конфигуратором» описана в документе «Конфигуратор СКУД Elsys. Руководство пользователя».

> ***Внимание!*** *После редактирования настроек оборудования следует запустить «Бастион-3 – Elsys» и выполнить обновление дерева устройств, запустив конфигуратор драйвера в «Бастион-3» и выполнив команду «Импорт из оборудования», после чего выполнить инициализацию измененных устройств.*

3.7.3 Настройка «Территорий»

Для работы глобального контроля последовательности прохода необходимо сконфигурировать «Территории» (Рис. 12).

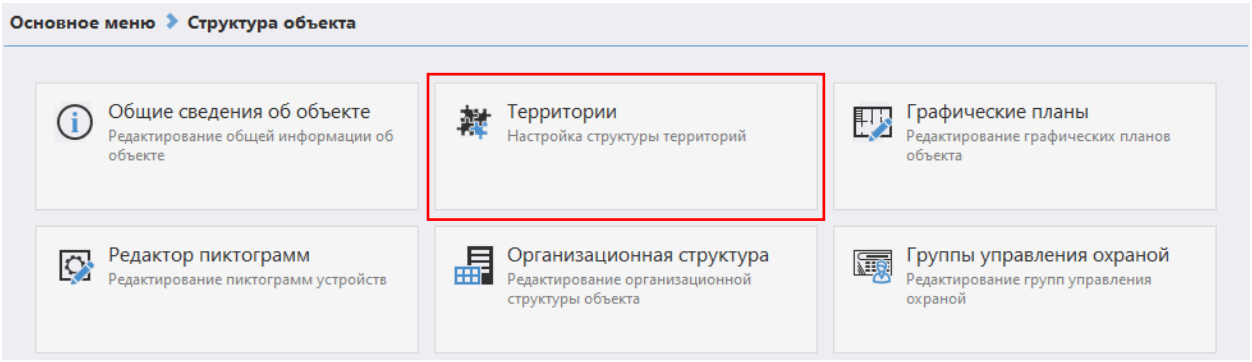


Рис. 12. Вызов окна настройки областей контроля

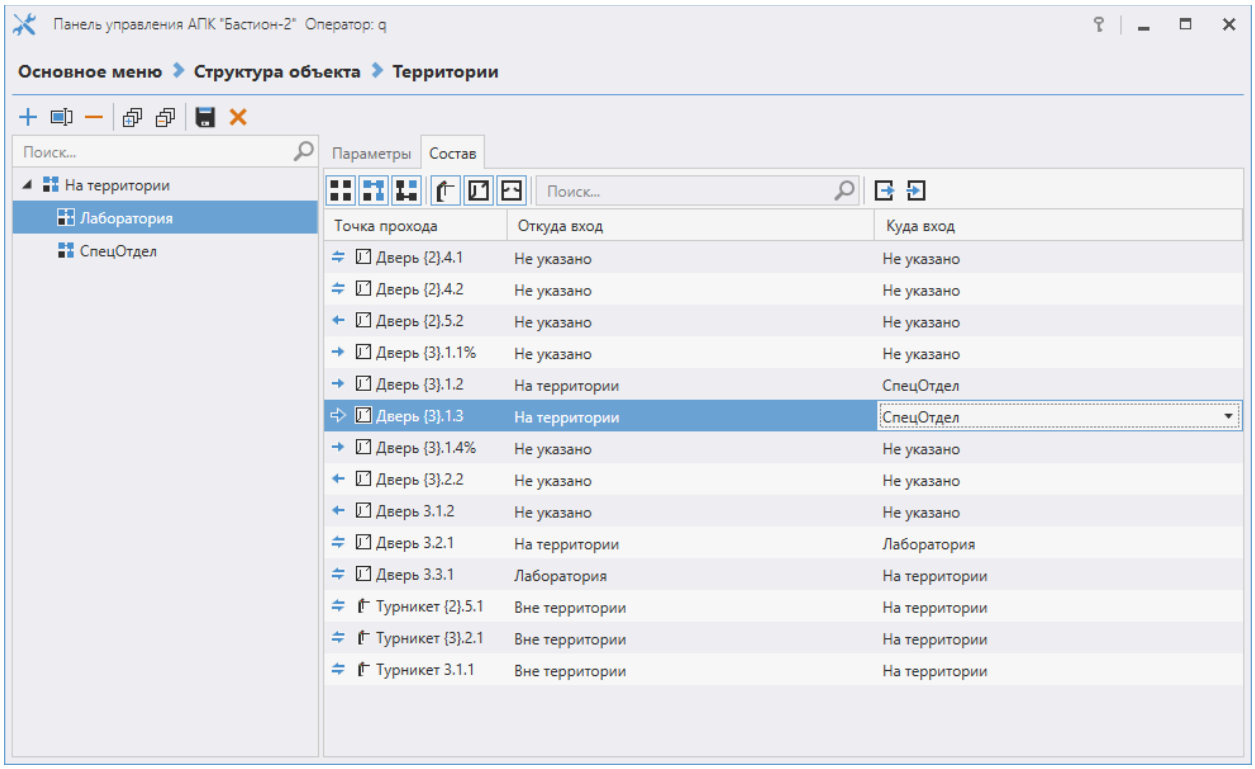


Рис. 13. Окно настройки областей контроля

В появившемся окне (Рис. 13) необходимо указать из какой и на какую «Территорию» ведет каждая точка доступа. На рисунке приведён пример настройки областей контроля для предприятия.

Подробное описание настройки областей контроля дано в «Бастион-3. Руководство администратора».

3.7.4 Дополнительные настройки глобального контроля последовательности прохода

3.7.4.1 Мягкий antipassback

Если при использовании контроля последовательности прохода необходимо, регистрируя нарушение, автоматически предоставлять доступ, следует в свойствах считывателей включить настройку **«Предоставлять доступ при нарушении зоны доступа»** (Рис. 14).

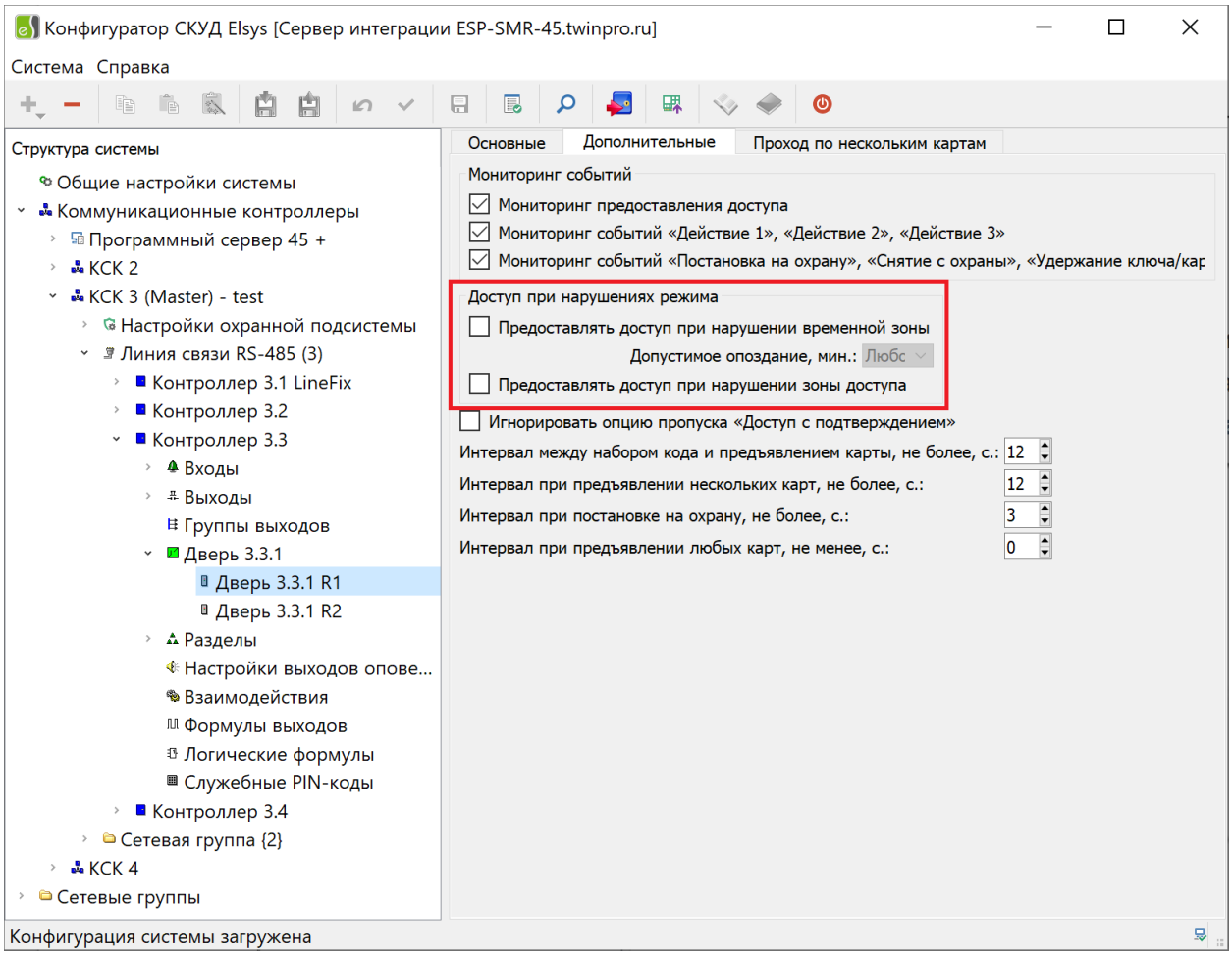


Рис. 14. Включение «мягкого» antipassback в автономном конфигураторе

Настройка вступает в силу после инициализации контроллеров доступа.

3.7.4.2 Настройка «Сброс в полночь»

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

Это можно сделать, включив в контроллерах доступа, где это необходимо, настройку **«Сброс в полночь»** (Рис. 15).

Если эта настройка включена, то в 0 час 0 мин ежесуточно в контроллерах будет очищаться информация о текущей зоне доступа всех пропусков.

3.7.4.3 Временной antipassback

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

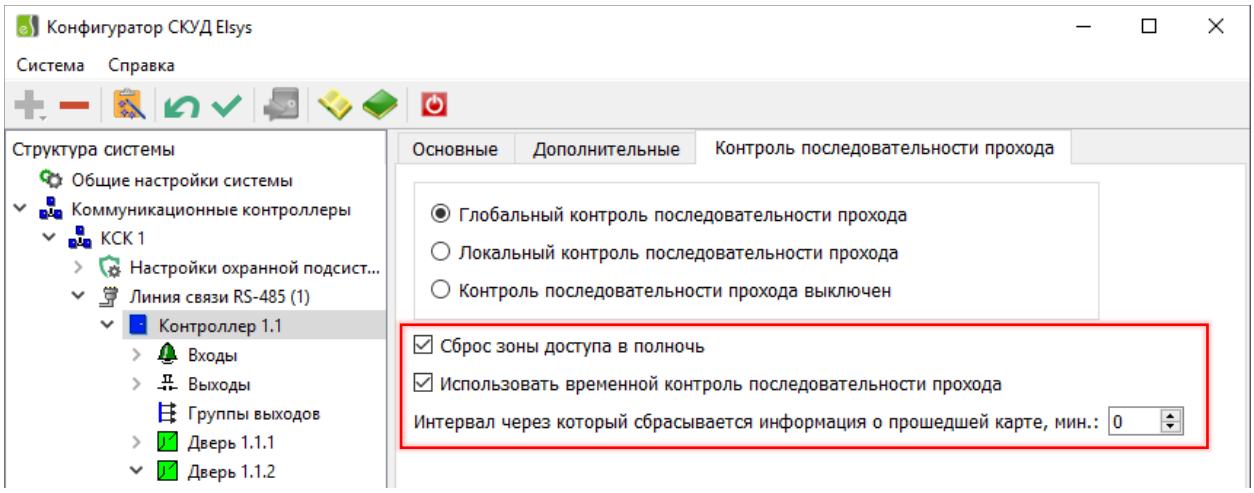


Рис. 15. Настройка «Сброс в полночь» и «Временной antipassback» в автономном конфигураторе

Режим временного контроля последовательности прохода может быть включен для контроллеров старших моделей (Light, Standard, Pro, Pro4), имеющих номер версии встроенного ПО 2.53 или старше и установленный модуль расширения памяти. Кроме того, для работы этого режима должна быть включена опция контроллера **«Использовать временный контроль последовательности прохода»** (Рис. 15) и задана настройка **«Интервал, через который сбрасывается информация о прошедшей карте, мин»**.

Описанные настройки вступают в силу после инициализации контроллеров 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), а также в некоторых других случаях.

3.7.4.4 Настройка «Не проверять исправность областей контроля»

Настройка **«Не проверять исправность областей контроля»** (Рис. 16) определяет алгоритм работы функции antipassback при потерях связи с контроллерами.

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

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

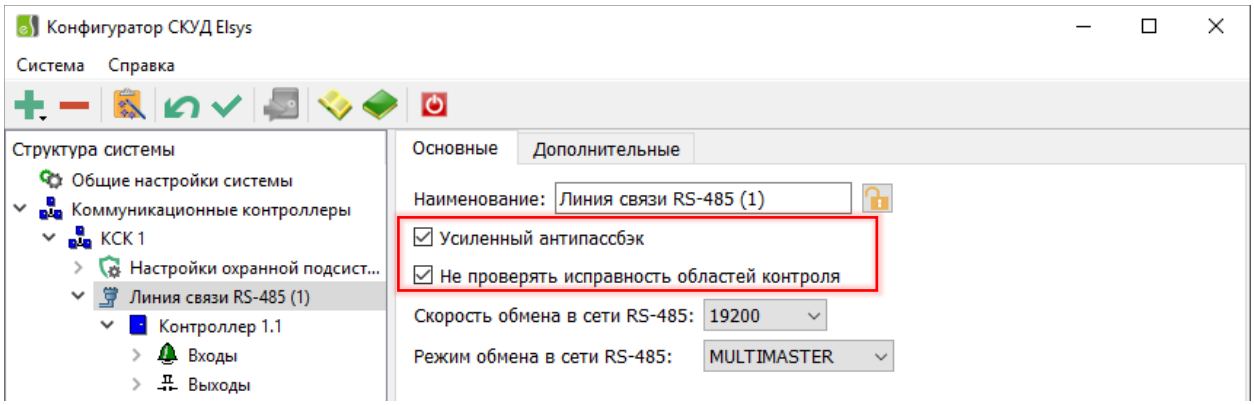


Рис. 16. Настройка «Усиленный антипассбэк» и «Не проверять области контроля» в автономном конфигураторе

Если настройка **«Не проверять исправность областей контроля»** включена, сброс текущего местоположения пользователей при нарушениях связи не выполняется. Тем самым обеспечивается сохранение работоспособности функции antipassback при кратковременных и длительных нарушениях связи, однако становятся возможными необоснованные отказы в доступе.

В конфигураторе СКУД Elsys настройка **«Не проверять исправность областей контроля»** присутствует в окнах свойств линии связи RS-485 коммуникационного сетевого контроллера и сетевой группы. Настройка вступает в силу после инициализации всех контроллеров Elsys-MB, относящихся к соответствующим линиям связи или сетевым группам, и после инициализации всех КСК Elsys-MB-Net, где она была изменена.

3.7.4.5 Настройка «Усиленный antipassback»

«Усиленный antipassback» – режим, обеспечивающий дополнительную защиту от несанкционированного доступа (Рис. 16). Суть его заключается в следующем. В обычном режиме (если настройка **«Усиленный antipassback»** выключена) сообщения об изменении зоны доступа рассылаются другим контроллерам после регистрации фактического прохода (в момент срабатывания датчика прохода). Нарушитель может, успев за время, отводимое на проход, предъявить на проходной карту нескольким считывателям, провести на территорию предприятия посторонних лиц. Для предотвращения такой ситуации можно настроить систему, чтобы проход регистрировался одновременно с предъявлением карты. Но в этом случае, сотруднику, предъявившему карту, но по каким-то причинам не успевшему совершить проход, в следующий раз в доступе будет отказано. Режим «Усиленный antipassback», будучи свободным от этого недостатка, предотвращает проход нескольких лиц по одной карте. В момент предъявления карты контроллер передаёт сообщение об изменении её текущей зоны доступа, а если проход не состоялся – сообщение о восстановлении текущей зоны доступа.

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

В конфигураторе СКУД Elsys настройка **«Усиленный antipassback»** присутствует в свойствах линии связи RS-485 коммуникационного сетевого контроллера и сетевой группы.

3.7.4.6 Индивидуальная настройка «не отслеживать последовательность прохода»

Для отдельных пользователей системы (VIP-персоны, персонал, по служебной необходимости совершающий перемещения вне точек доступа, и т. п.) antipassback может быть отключен установкой индивидуальной опции пропуска **«Не отслеживать последовательность прохода»** на вкладке **«Пропуск»** (Рис. 17).

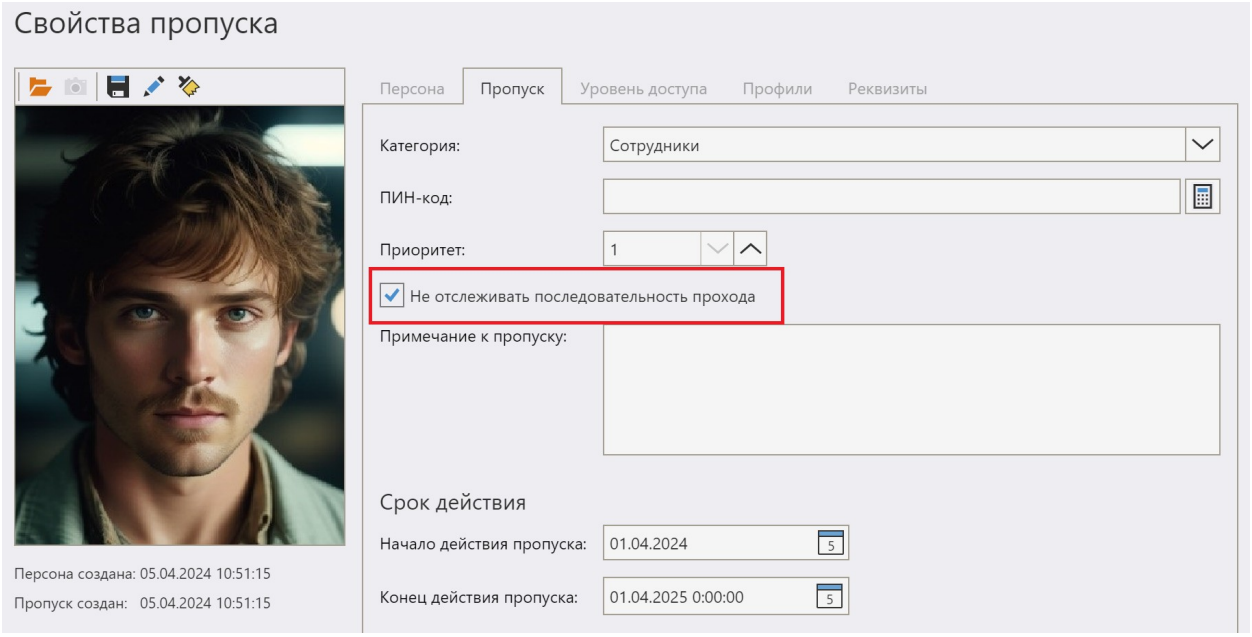


Рис. 17. Настройка «Не отслеживать последовательность прохода» в свойствах пропуска

3.8 Дополнительные настройки драйвера

3.8.1 Профили настроек персонала

В СКУД Elsys для каждого пропуска могут быть заданы дополнительные полномочия с помощью профилей настроек персонала.

Профиль настроек персонала в СКУД Elsys представляет собой совокупность аппаратных настроек контроллеров, которые можно назначить одному и нескольким пропускам.

Для настройки профилей используется конфигуратор, который вызывается с помощью кнопки **«Профили настройки персонала»** на ленте управления драйвера (Рис. 2).

Пользовательский интерфейс конфигуратора профилей персонала представлен на Рис. 18.

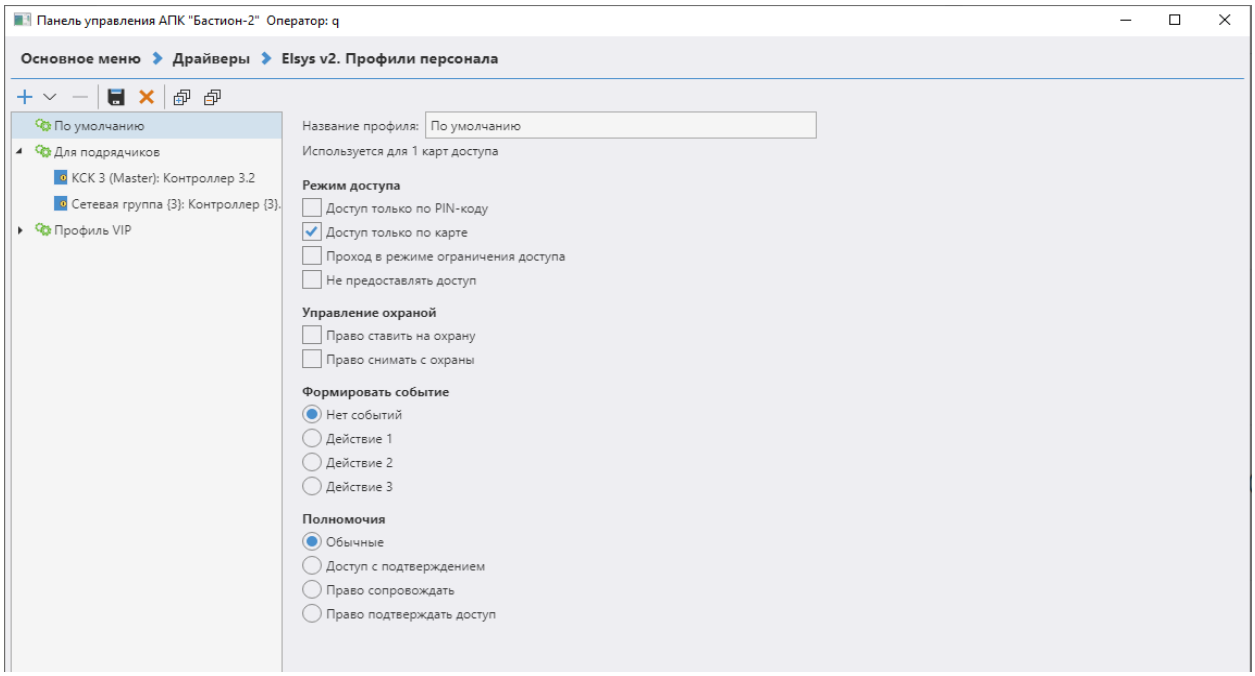
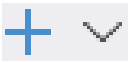


Рис. 18. Окно конфигуратора профилей персонала

Описание кнопок панели управления конфигуратора профилей приведено в Табл. 1.

Табл. 1. Назначение кнопок панели управления конфигуратора профилей персонала

Кнопка	Наименование	Назначение
	**«Добавить»**	Добавляет новый профиль или элемент профиля в конфигурацию. Функция также доступна из контекстного меню дерева конфигурации.
	«Удалить»	Удаляет существующие профиль или элемент профиля из конфигурации. Функция также доступна из контекстного меню выбранного узла. Функция недоступна для предопределённых профилей, а также для профилей, которые используются хотя бы одним пропуском.
	**«Отменить»**	Отменить внесённые изменения. Выполняется загрузка последней сохранённой конфигурации из базы данных.
	**«Сохранить»**	Сохранить внесённые изменения. Выполняется сохранение конфигурации в базу данных.
	**«Развернуть»**	Разворачивает все узлы дерева конфигурации.
	**«Свернуть»**	Сворачивает все узлы дерева конфигурации.

В левой части окна конфигуратора расположено дерево профилей настроек персонала, в котором имеется два типа узлов: узлы профилей и дочерние для них узлы (элементы профилей). В правой части окна расположена панель, предназначенная для настройки и просмотра свойств узла.

Изначально существует три предопределённых профиля, которые назначаются по умолчанию пропускам в бюро пропусков в соответствии с их типом:

- Профиль «Для постоянных карт»;
- Профиль «Для временных карт»;
- Профиль «Для разовых карт».

Предопределённые профили удалить нельзя, а их наименование недоступно для редактирования. Все остальные функции доступны как для обычных профилей, добавленных пользователем.

Конфигуратор профилей персонала позволяет создавать новые профили персонала, устанавливать настройки профилей по умолчанию (Ошибка: источник перекрёстной ссылки не найден), добавлять в профили дочерние элементы (контроллеры) и устанавливать для них собственные настройки (Рис. 20).

Добавленный пользователем профиль может быть в дальнейшем назначен любому пропуску. Добавленный пользователем профиль можно удалить, если он не назначен ни одному пропуску.

Настройки профиля и настройки элемента профиля – контроллера, идентичны по составу. Их описание приводится ниже.

«Доступ только по PIN-коду» и **«Доступ только по карте»** – эти настройки определяют, какие устройства используются для идентификации пользователя. Если обе опции выключены, и точка доступа оборудована считывателем и клавиатурой, для предоставления доступа необходимо набрать PIN-код и предъявить карту. Если включена первая опция, то для получения доступа достаточно набрать PIN-код, а если включена вторая – достаточно предъявить карту.

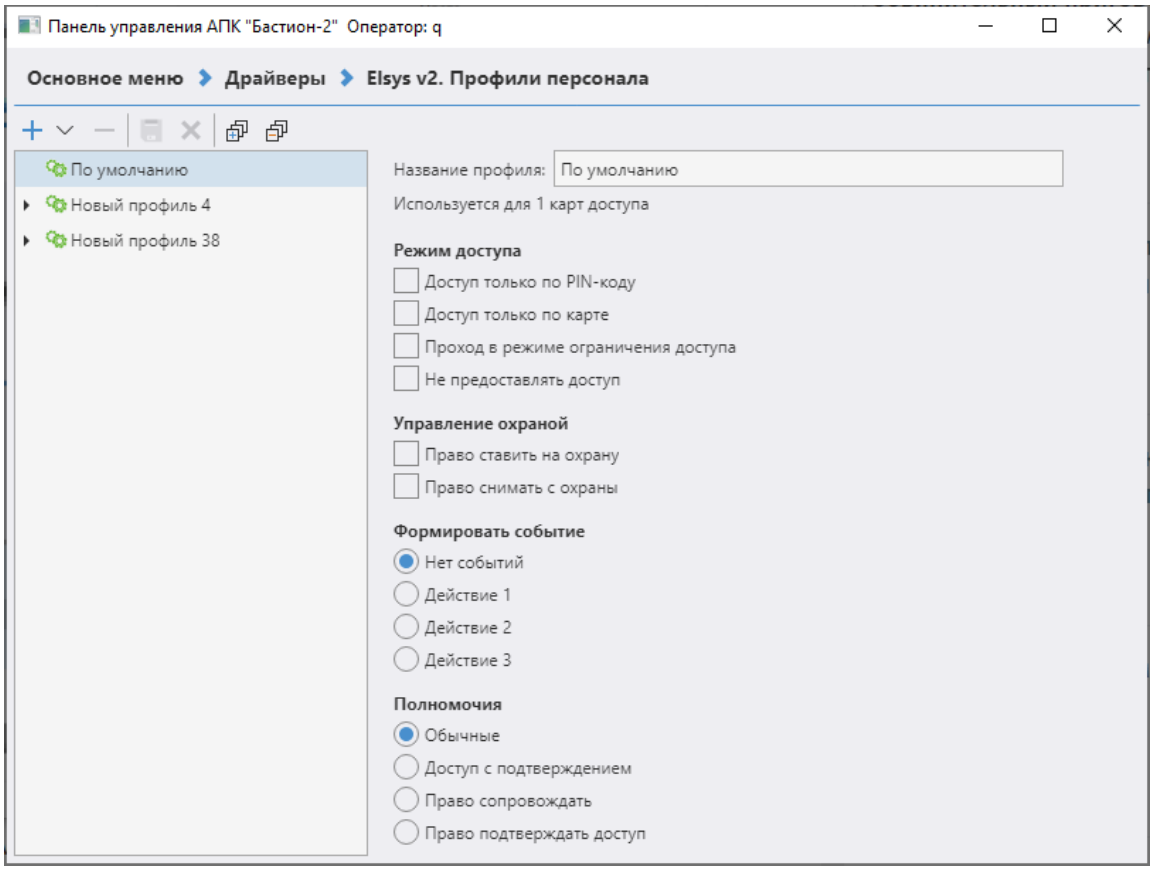


Рис. 19. Настройки профиля по умолчанию

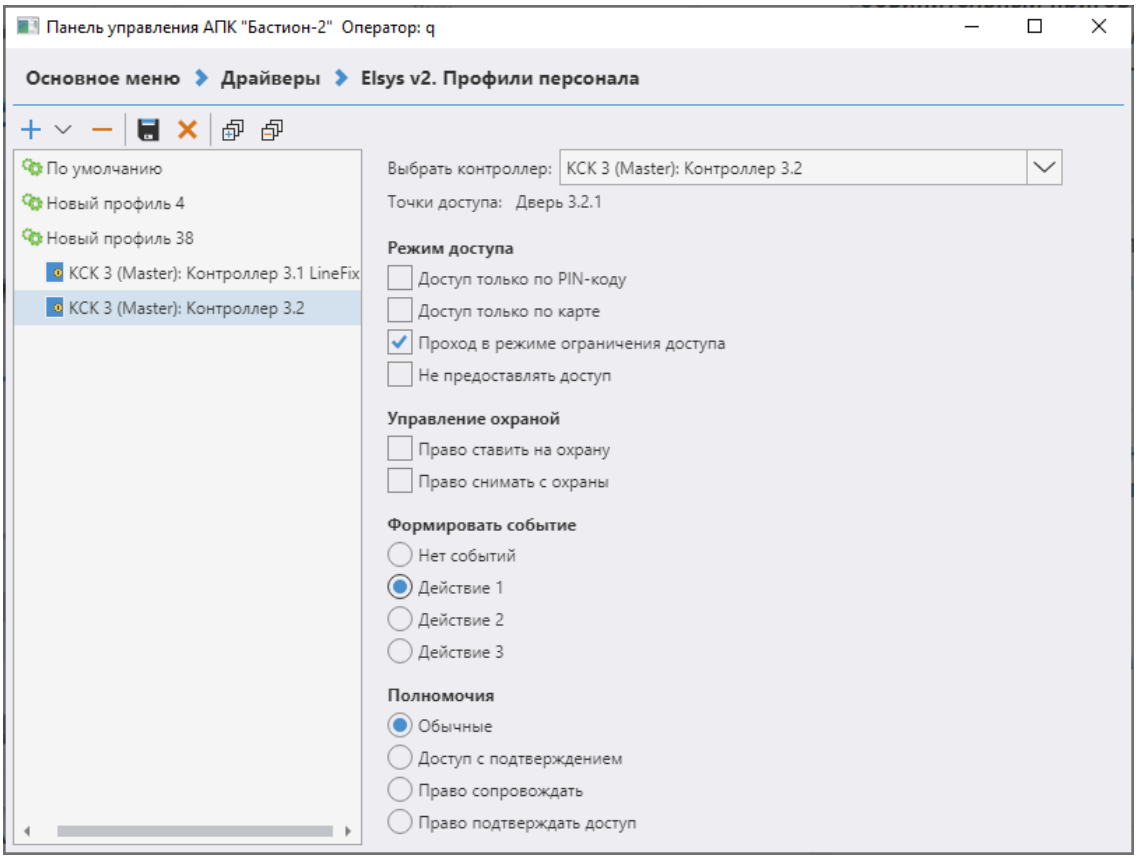


Рис. 20. Настройки элемента профиля

«Проход в режиме ограничения доступа» – эта настройка позволяет получать разрешение на проход, если считыватель находится в режиме ограничения доступа.

«Не предоставлять доступ» – если эта опция включена, то карта может использоваться только для управления охраной и выполнения других действий. Доступ не предоставляется.

«Право ставить на охрану» и **«Право снимать с охраны»** – эти опции позволяют выполнять пользователю действия по управлению охраной с помощью кнопки управления охраной (Рис. 21).

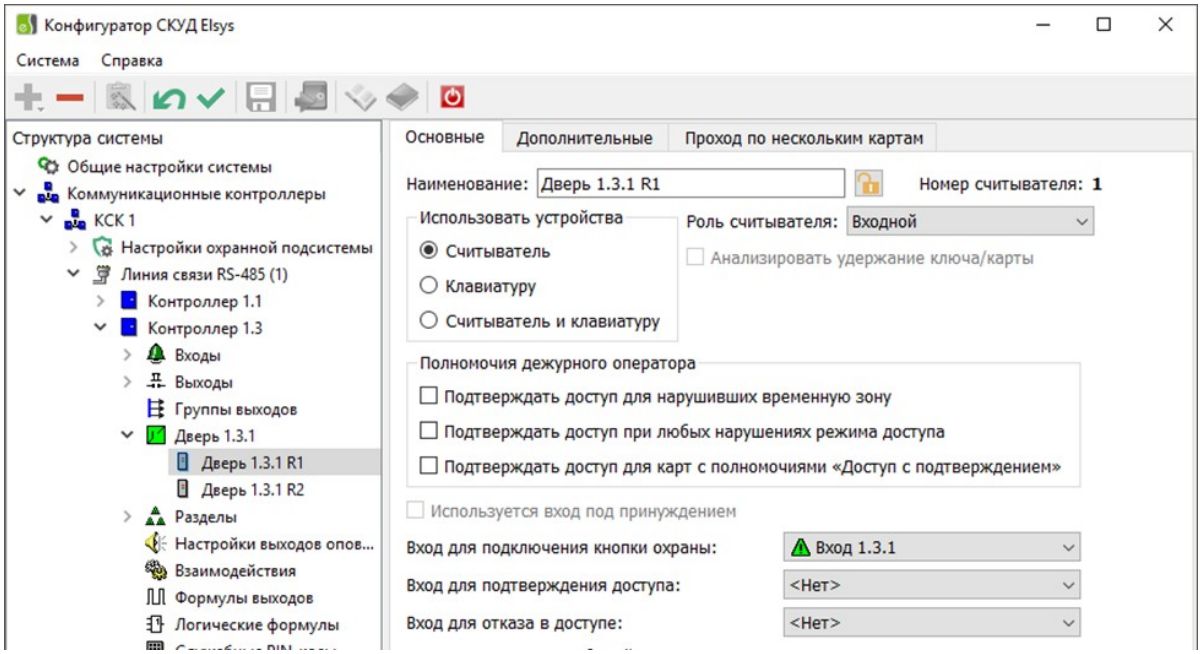


Рис. 21. Вход управления охраной в автономном конфигураторе

Опция **«Право ставить на охрану»**, кроме того, разрешает сотруднику использование служебных PIN-кодов (Рис. 22).

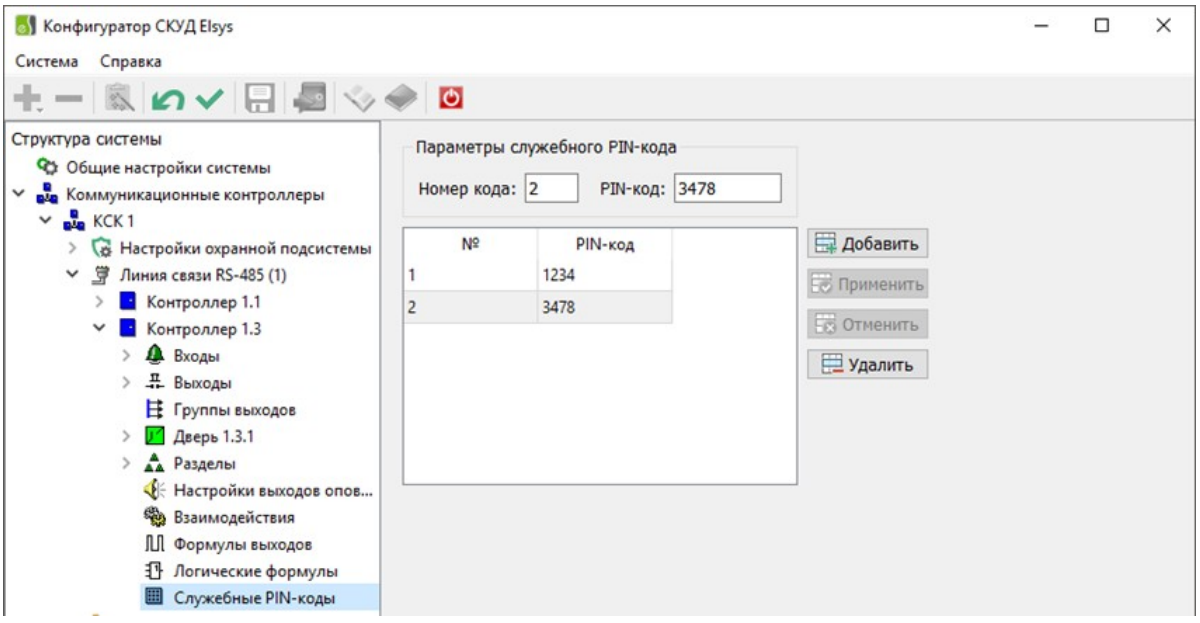


Рис. 22. Настройка служебных PIN-кодов в автономном конфигураторе

«Формировать событие» – если выбрано одно из событий (действие 1, действие 2, действие 3), то при предъявлении карты будут обрабатываться взаимодействия, назначенные на это событие считывателя.

Группа настроек **«Полномочия»**. По умолчанию – **«Обычные»**. Если установлены полномочия **«Доступ с подтверждением»**, то для предоставления доступа необходимо вслед за предъявлением данной карты предъявить карту с полномочиями **«Право сопровождать»** или **«Право подтверждать доступ»**.

Различие между последними двумя полномочиями в том, что картам с полномочиями «Право сопровождать» при подтверждении доступа также предоставляется доступ (система зафиксирует проход двух сотрудников), а картам с полномочиями «Право подтверждать доступ» – нет (будет зафиксирован проход первого сотрудника). Во всём остальном права этих двух групп полномочий соответствуют полномочиям «Обычные». Если для считывателя включена опция «Подтверждать доступ для карт, требующих подтверждения», то для карт с полномочиями «Доступ с подтверждением» подтверждение осуществляется только кнопкой дежурного оператора «Подтверждение доступа».

Если назначенный пропуску профиль не имеет дочерних элементов, то для всех точек доступа, входящих в уровень доступа пропуска, действуют настройки профиля по умолчанию.

Если назначенный пропуску профиль содержит контроллеры, то для точек доступа, подключенных к этим контроллерам и входящих в уровень доступа, пропуска действуют настройки соответствующих контроллеров, для остальных точек доступа действуют настройки профиля по умолчанию.

В бюро пропусков по умолчанию для пропуска задаётся профиль в соответствии с его типом: для постоянных пропусков задаётся профиль «Для постоянных карт», для временных пропусков – профиль «Для временных карт», для разовых пропусков - профиль «Для разовых карт».

Изменить назначенный пропуску профиль можно в бюро пропусков, указав в свойствах пропуска на вкладке «Профили» заранее подготовленный в конфигураторе профилей требуемый профиль (Рис. 23).

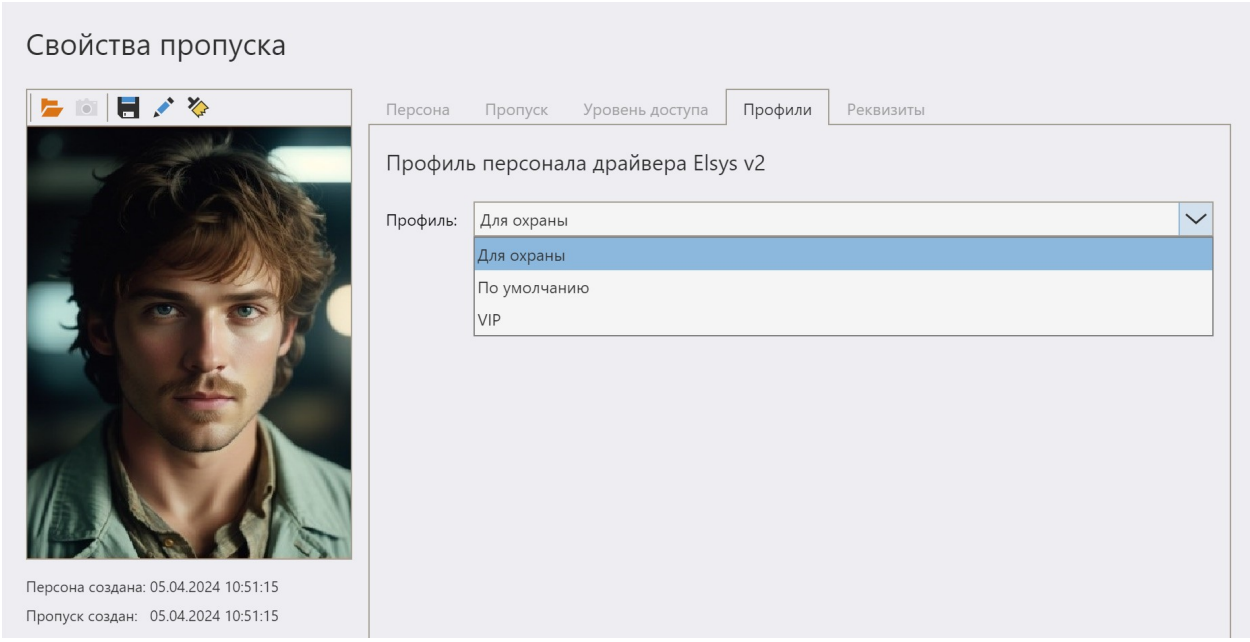


Рис. 23. Назначение пропуску персоны профиля «Для охраны»

Назначаемые профили по умолчанию для каждой категории пропусков можно изменить, выбрав в «Панели управления» в разделе «Пропускной режим» - «Категории пропусков» закладку **«Профили СКУД»**.

На Рис. 24 показано назначение пропускам категории «Сотрудники» профиля «Для сотрудников».

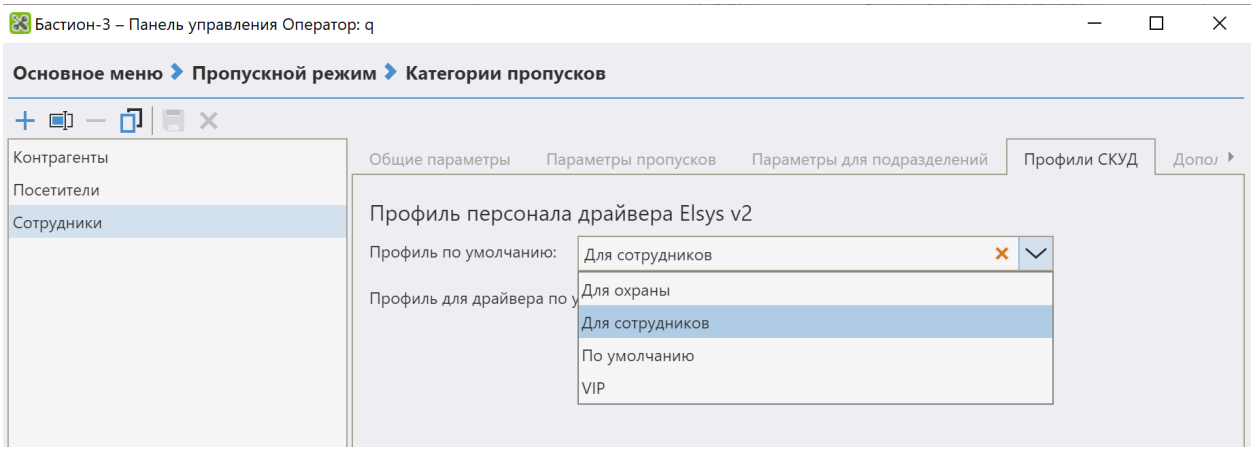


Рис. 24. Назначение профиля «Для сотрудников» по умолчанию для категории пропусков

3.8.2 Автоматическая постановка раздела на охрану при выходе последнего сотрудника

Для того, чтобы использовать эту функцию, необходимо включить одноимённую опцию раздела (**«Автоматическая постановка на охрану при выходе последнего сотрудника»** на Рис. 25).

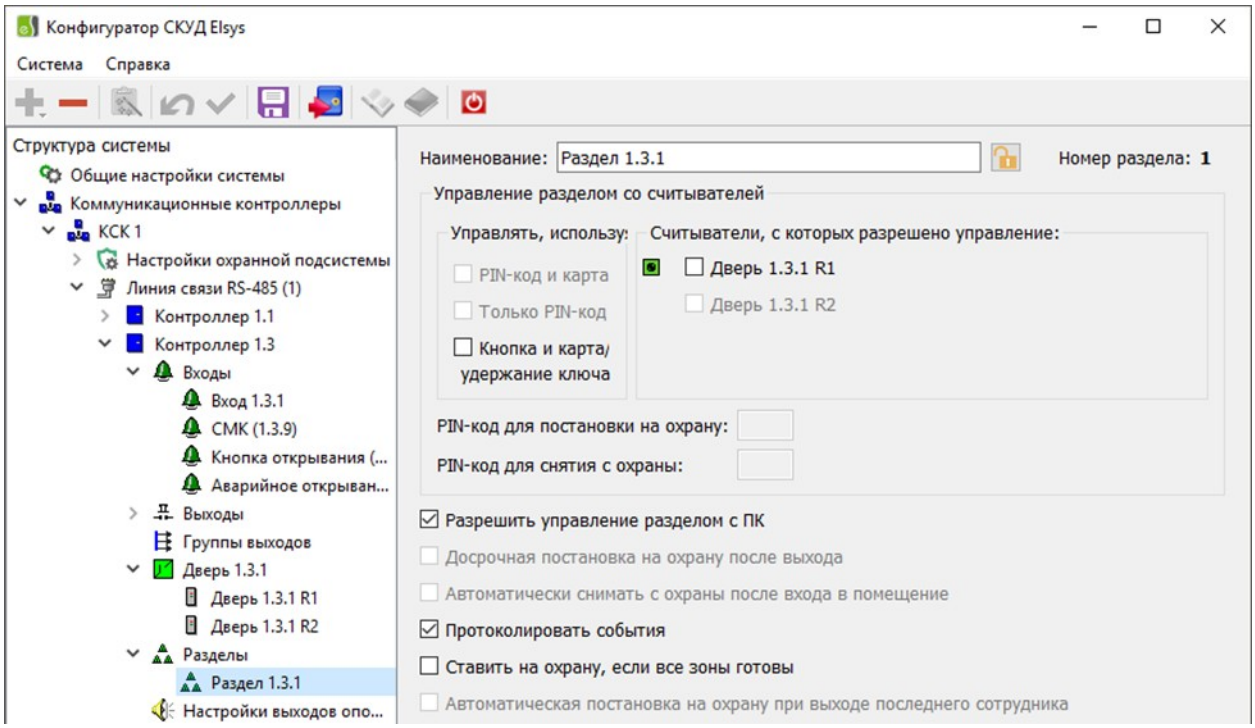


Рис. 25. Настройка разделов в автономном конфигураторе

Эта функция может быть включена только для одного раздела, содержащего в своем составе одну или две двусторонние двери. Если дверь, входящая в раздел, участвует в глобальном контроле последовательности прохода, необходимо выполнение следующих условий:

- для двери, входящей в раздел, должны быть настроены внешняя и внутренняя зоны доступа (при этом они не должны совпадать);
- во внутреннюю зону доступ должен осуществляться только через дверь (двери), входящую в раздел. Никакие другие точки доступа не должны граничить с внутренней зоной доступа, ни в этом, ни в других контроллерах.

Если глобальный контроль последовательности прохода в этом контроллере не используется, никаких дополнительных настроек не нужно.

При использовании автоматической постановки последним выходящим сотрудником

рекомендуется выполнить следующие настройки:

- для входного ШС (двери) установить задержку взятия;

- для остальных ШС, исключая объемные, установить опцию **«Автоматическая постановка на охрану из состояния «Не взято»** (Рис. 26);

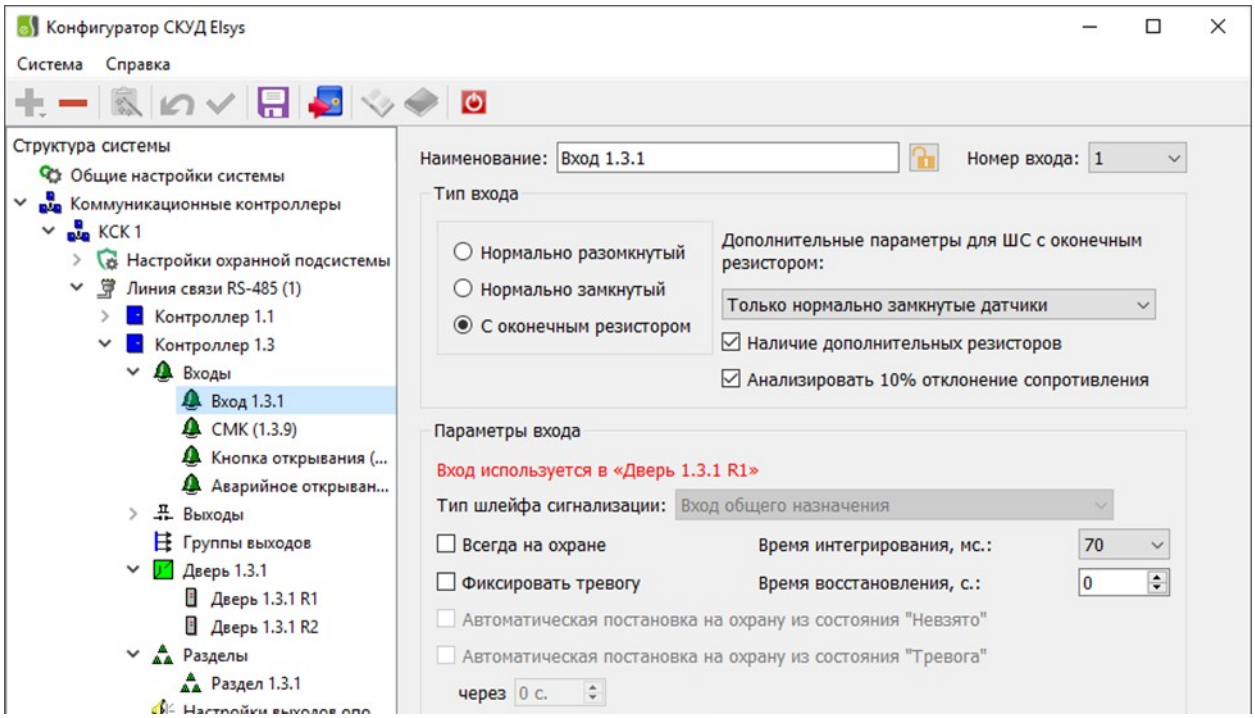


Рис. 26. Настройка охранных входов в автономном конфигураторе

- для раздела выключить настройку **«Ставить на охрану, если все зоны готовы»**;
- включить настройку раздела **«Автоматическое снятие с охраны при входе в помещение»**;
- включить настройку **«Досрочная постановка на охрану после выхода»** (это нужно, чтобы последний выходящий сотрудник успел проконтролировать, все ли ШС, входящие в раздел, поставлены на охрану).

Такое сочетание настроек гарантирует автоматическую постановку раздела на охрану при любых состояниях охранных ШС и автоматическое снятие помещения с охраны при входе в помещение.

При использовании автоматической постановки на охрану подсчёт числа сотрудников в помещении будет выполняться после каждого события «Штатный вход» или «Штатный выход», зарегистрированного на двери, входящей в состав раздела. При подсчёте числа сотрудников учитывается текущее местоположение каждого пользователя, а не общее число событий «Штатный вход/выход» что существенно повышает точность подсчёта количества сотрудников.

При постановке раздела на охрану счётчик персонала автоматически сбрасывается (устанавливается в нуль). После снятия раздела с охраны контроллер после каждого прохода обновляет счётчик персонала. В момент выхода последнего сотрудника (соответствует моменту регистрации события «Штатный выход», формируемого

одновременно с открыванием двери), осуществляется автоматическая постановка раздела на охрану. По истечении 5 с после закрывания двери (если включена настройка **«Досрочная постановка на охрану после выхода»**) выполнится досрочная постановка всех ШС раздела на охрану.

Если по истечении времени задержки взятия объемные и входные ШС будут в нарушенном состоянии, будет сформирована тревога. Если ШС имеет включенную опцию **«Автоматическая постановка на охрану из состояния «Не взято»**, он в случае неготовности в момент постановки на охрану будет пребывать в состоянии «Невзятие» до тех пор, пока не восстановится его нормальное состояние. Поэтому, если по истечении 5 с после закрытия двери, раздел полностью не поставлен на охрану, сотрудник должен вручную снять раздел с охраны и устранить причину неготовности охранных ШС. Раздел должен быть снят с охраны до окончания времени задержки взятия входного ШС, в противном случае будет сформирована тревога. О наличии нарушенных ШС после выхода из помещения можно узнать по световой и звуковой индикации считывателей, а также по миганию светового оповещателя «Лампа».

Поставленный на охрану раздел снять с охраны имеют право только пользователи, имеющие полномочия «Снятие с охраны». Это условие актуально и в случае, если включена настройка **«Автоматическое снятие с охраны при входе в помещение»**. Для всех остальных сотрудников, которым не назначены полномочия «Снятие с охраны», доступ в охраняемое помещение будет ограничен.

Следует помнить, что автоматическая постановка на охрану при выходе последнего выходящего сотрудника является функцией, повышающей удобство пользования системой, но не должна рассматриваться как единственный способ управления режимами охраны. Возможен ряд ситуаций, в которых необходимо вмешательство дежурного оператора или пользователя.

Некоторые из возможных ситуаций приведены в Табл. 2.

Табл. 2. Описание ситуаций, требующих вмешательства дежурного оператора при автоматической постановке на охрану

№	Описание ситуации	Причины	Способ решения
1	Контроллер считает, что выходит последний сотрудник, в то время как в помещении остались люди	Произошёл сбой при подсчёте людей по причине того, что кто-либо из находящихся в помещении вошёл без карты либо предъявил карту на выход, но не вышел (например, чтобы впустить посетителя, не имеющего карты). Помещение будет поставлено на охрану, а в помещении будут находиться все нарушители	Поскольку в помещении остались люди, и они же являются нарушителями пропускного режима, ошибочная постановка помещения на охрану будет замечена. Необходимо снять помещение с охраны, в течение действия времени задержки взятия. И затем, при выходе последнего сотрудника, – вручную поставить помещение на охрану.

№	Описание ситуации	Причины	Способ решения
		пропускного режима.	
2	Вышел последний сотрудник, в то время как контроллер считает, что в помещении остались люди	Произошёл сбой при подсчёте людей по причине того, что кто-либо из сотрудников вышел вслед за другим, не отметившись на выходном считывателе. Либо (что менее вероятно) кто-либо предъявил карту на вход, открыл дверь, но не вошёл. Помещение не будет поставлено на охрану.	Если сотрудник, совершающий выход из помещения, точно знает, что больше в помещении никого нет, он должен вручную поставить помещение на охрану. По отсутствию характерной звуковой индикации на считывателе и световой – на оповещателе «Лампа», сотрудник должен определить, что отсутствовала попытка постановки на охрану.
3	Неудачная постановка на охрану при выходе последнего выходящего сотрудника	Неготовность охранных ШС в составе раздела	При выходе из помещения сотрудник, обнаружив, что выполняется автоматическая постановка на охрану, должен дождаться полной постановки раздела на охрану. Если по истечении 5 с после закрытия двери раздел полностью не поставлен на охрану, сотрудник должен снять раздел с охраны, совершив вход в помещение, и устранить причину неготовности охранных ШС.

3.8.3 Порты, используемые КСК Elsys-MB-Net и контроллерами Elsys-MB-IP

Информация, приведённая в настоящей главе, может потребоваться для настройки системы, если в локальной сети используются брандмауэры или сетевые экраны.

Структурная схема, иллюстрирующая взаимодействие КСК Elsys-MB-Net и контроллеров Elsys-MB-IP между собой и с программным обеспечением «Бастион-3» изображена на Рис. 27.

В Табл. 3 перечислены порты протоколов TCP/IP и UDP/IP, используемые коммуникационными сетевыми контроллерами Elsys-MB-Net.

В Табл. 4 перечислены порты протокола UDP/IP, используемые модулями Elsys-IP при обмене данными.

Все порты, перечисленные в Табл. 3, Табл. 4, должны быть разрешены для свободного обмена данными.

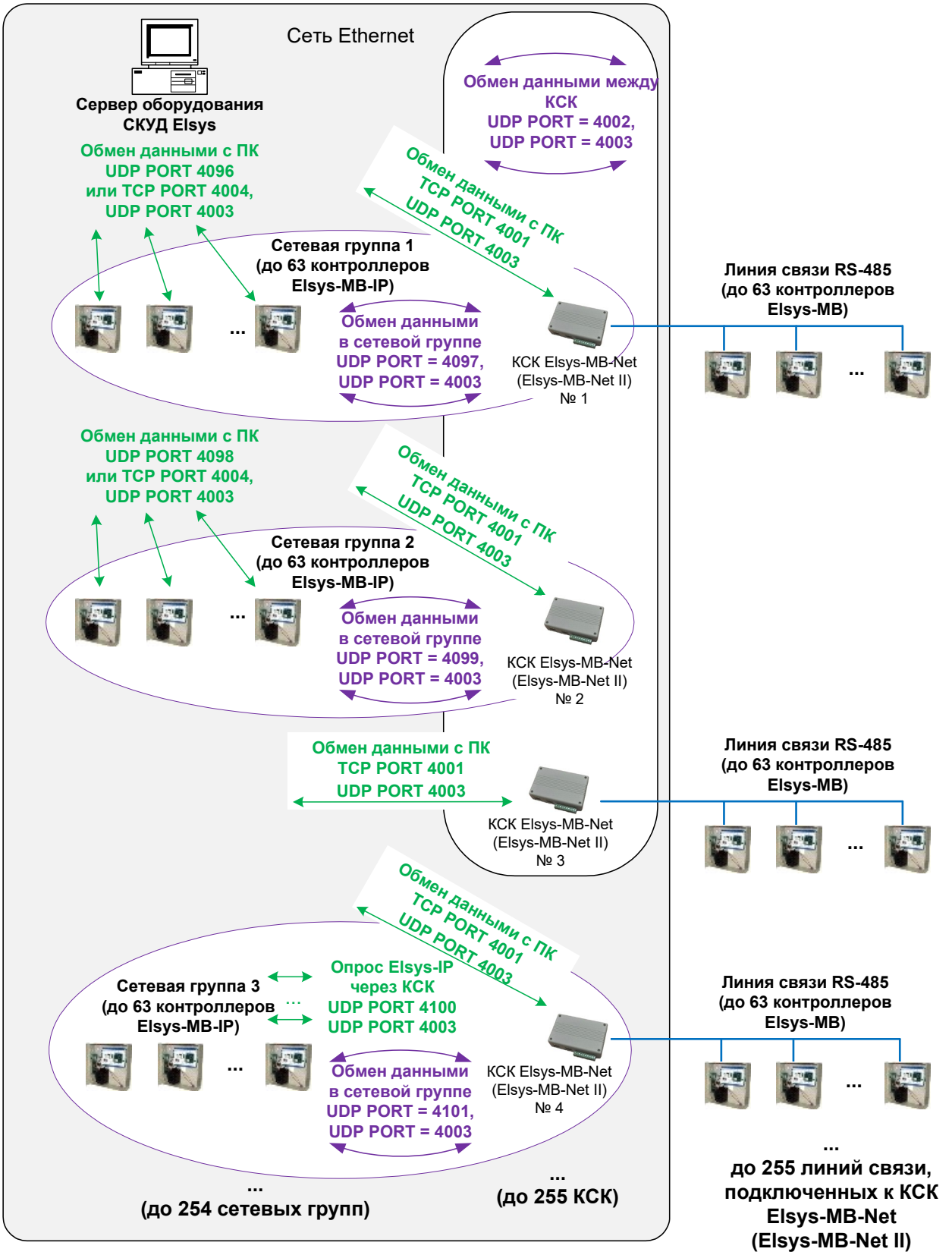


Рис. 27. Организация информационного обмена в СКУД Elsys с участием КСК Elsys-MB-Net и контроллеров Elsys-IP

Табл. 3. Порты протоколов TCP/IP и UDP/IP, используемые КСК Elsys-MB-Net

№ порта	Тип порта	Назначение порта
4001	TCP	Используется для обмена данными между управляющим ПО и КСК Elsys-MB-Net. КСК является TCP-сервером, ПК – TCP-клиентом. КСК поддерживает только одно TCP-соединение
4002	UDP	Используется для обмена данными между КСК для обеспечения функции «Глобальный контроль последовательности прохода». По этому порту могут, в зависимости от режима работы, передаваться адресные и широковещательные UDP-дейтаграммы (с широковещательным адресом 255.255.255.255 или с адресом подсети).
4003	UDP	Используется для обмена широковещательными дейтаграммами с ПК при поиске оборудования и назначении сетевых настроек, а также для проверки связи с другими КСК Elsys-MB-Net и контроллерами Elsys-MB-IP.
4004	UDP	*Не используется* *(использовался в версиях КСК Elsys-MB-Net ниже 2.08 для проверки связи с другими КСК)*
4096 + (N – 1)*2 + 1	UDP	Порт используется для обмена данными с контроллерами Elsys-MB-IP, если КСК включён в сетевую группу. По этому порту могут, в зависимости от режима работы, передаваться адресные и широковещательные (с широковещательным адресом 255.255.255.255 или с адресом подсети) UDP-дейтаграммы. Номер порта вычисляется по указанной формуле, где N – номер сетевой группы. Так, для сетевой группы 1 будет использоваться порт 4097, для сетевой группы 2–4099, для сетевой группы 10 – порт 4115 и т. д.

Табл. 4. Порты протокола UDP/IP, используемые модулем Elsys-IP

№ порта	Назначение порта
4096 + (N – 1)*2	Порт используется для обмена данными между управляющим ПО и контроллерами Elsys-MB-IP. По этому порту передаются адресные UDP-дейтаграммы. Номер порта вычисляется по указанной формуле, где N – номер сетевой группы. Так, для сетевой группы 1 будет использоваться порт 4096, для сетевой группы 2–4098, для сетевой группы 10 – порт 4114 и т. д.
4096 + (N – 1)*2 + 1	Порт используется для обмена данными между контроллерами Elsys-MB-IP. По этому порту могут, в зависимости от режима работы, передаваться адресные и широковещательные (с широковещательным адресом

№ порта	Назначение порта
	255.255.255.255 или с адресом подсети) UDP-дейтаграммы. Номер порта вычисляется по указанной формуле, где N – номер сетевой группы. Так, для сетевой группы 1 будет использоваться порт 4097, для сетевой группы 2 – 4099, для сетевой группы 10 – порт 4115 и т. д.
4003	Используется для обмена широковещательными дейтаграммами с ПК при поиске оборудования и назначении сетевых настроек, а также для проверки связи с другими контроллерами Elsys-MB-IP и КСК Elsys-MB-Net.

3.9 Порядок настройки СКУД Elsys для различных режимов работы

3.9.1 Общие настройки ПК «Бастион-3», используемые в работе драйвера

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

Для повышения точности протоколирования событий в общих настройках ПК «Бастион-3» рекомендуется настроить синхронизацию времени, как минимум, раз в сутки (см. «Руководство администратора»). При этом, в заданное время будет выполняться синхронизация часов рабочих станций и подключенного к ним оборудования.

3.9.2 Настройка системы при использовании двойной идентификации (PIN-код и карта)

Если в СКУД Elsys предполагается использовать PIN-коды, необходимо выполнить ряд настроек.

В настройках контроллера Elsys-MB любых вариантов исполнения, кроме SM, следует:

- включить опцию «Использовать PIN-коды»;
- задать тип используемых клавиатур (наиболее распространены клавиатуры, совмещённые со считывателем, предающие коды клавиш по интерфейсу Wiegand);
- при необходимости изменить настройку **«Завершать ввод PIN-кода символом */#»**.

В настройках считывателей (при настройке оборудования в «Автономном конфигураторе СКУД») необходимо задать, какие устройства будут использоваться для идентификации (считыватель, клавиатура, считыватель + клавиатура). Если предполагается использование режима **«Доступ под принуждением»**, следует включить у считывателя соответствующую настройку.

В свойствах пропуска (см. «Бюро пропусков. Руководство оператора») необходимо для каждого пользователя задать PIN-код. В драйвере Elsys допустимые значения PIN-кодов находятся в диапазоне от 1 до 65534. В бюро пропусков установлено ограничение от 1 до 9999.

3.9.3 Доступ с подтверждением картой

Доступ с подтверждением картой – встроенный усиленный алгоритм прохода, обеспечивающий для определённой категории пользователей СКУД (как правило, посетителей предприятия) доступ в отдельные точки прохода только в сопровождении лиц, уполномоченных подтверждать доступ.

На Рис. 28 показана последовательность регистрируемых событий при использовании доступа с подтверждением картой.

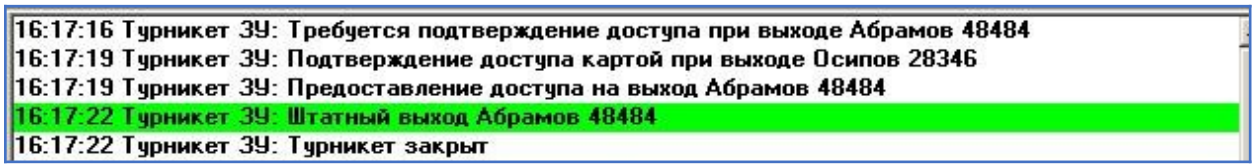


Рис. 28. Последовательность событий при использовании режима «Доступ с подтверждением картой»

Если в течение заданного времени (задаётся настройкой **«Интервал при предъявлении нескольких карт»** на вкладке свойств считывателя **«Дополнительные»**) подтверждающая карта не будет предъявлена, будет сформировано событие «Ошибка ввода второй карты».

Для реализации режима «Доступ с подтверждением картой» необходимо настроить персональные настройки двум категориям лиц, задав им соответственно полномочия **«Доступ с подтверждением»** и **«Право подтверждать доступ»** (см. Рис. 29, Рис. 30, Рис. 31). Для остальных сотрудников могут быть оставлены полномочия «Обычные».

Если нужно, чтобы система регистрировала также проход сотрудника, подтвердившего доступ, следует включить опцию **«Право сопровождать»** (однако, эту опцию не следует применять на турникетах, так как в этом случае одновременный проход двух сотрудников невозможен). Если нужно, чтобы подтверждающий пропуск не имел прав доступа, а использовался только для подтверждения доступа, необходимо для него включить опцию **«Не предоставлять доступ»** (обычно этот вариант используется на постах охраны).

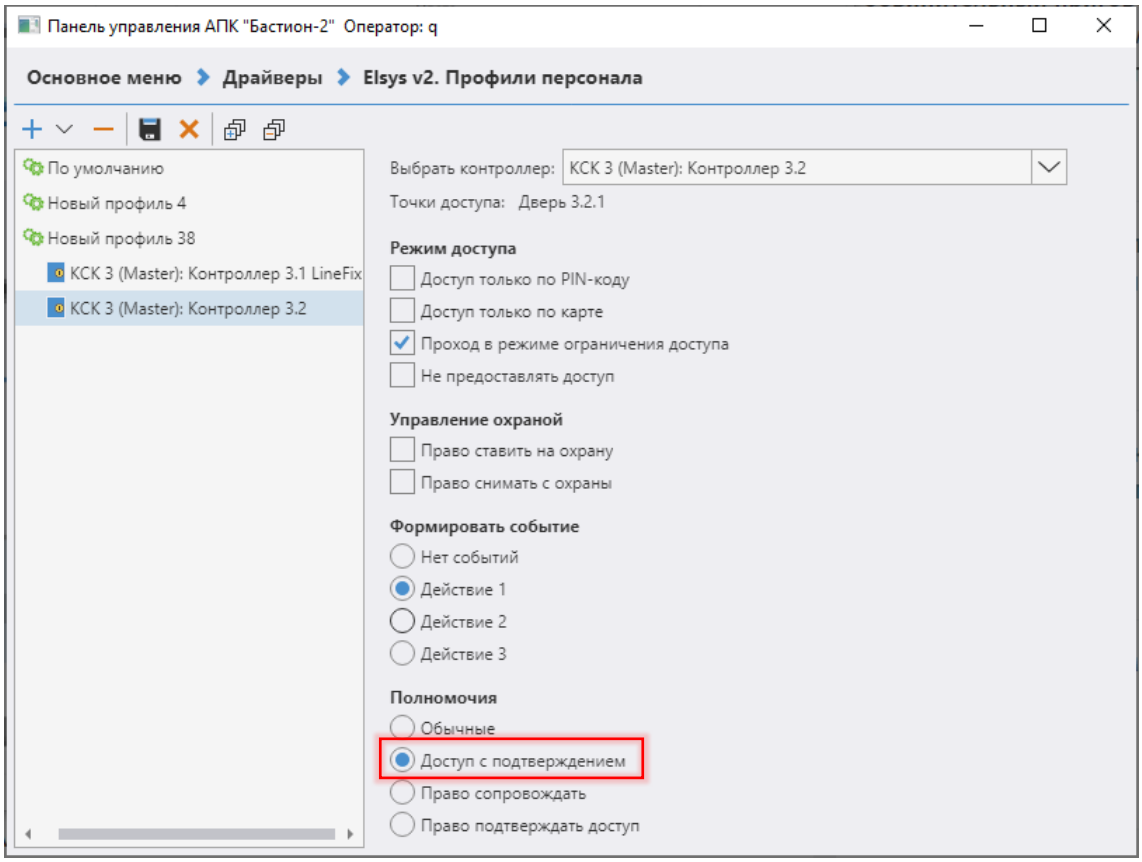


Рис. 29. Профиль настроек персонала для лиц, которым необходимо подтверждать доступ

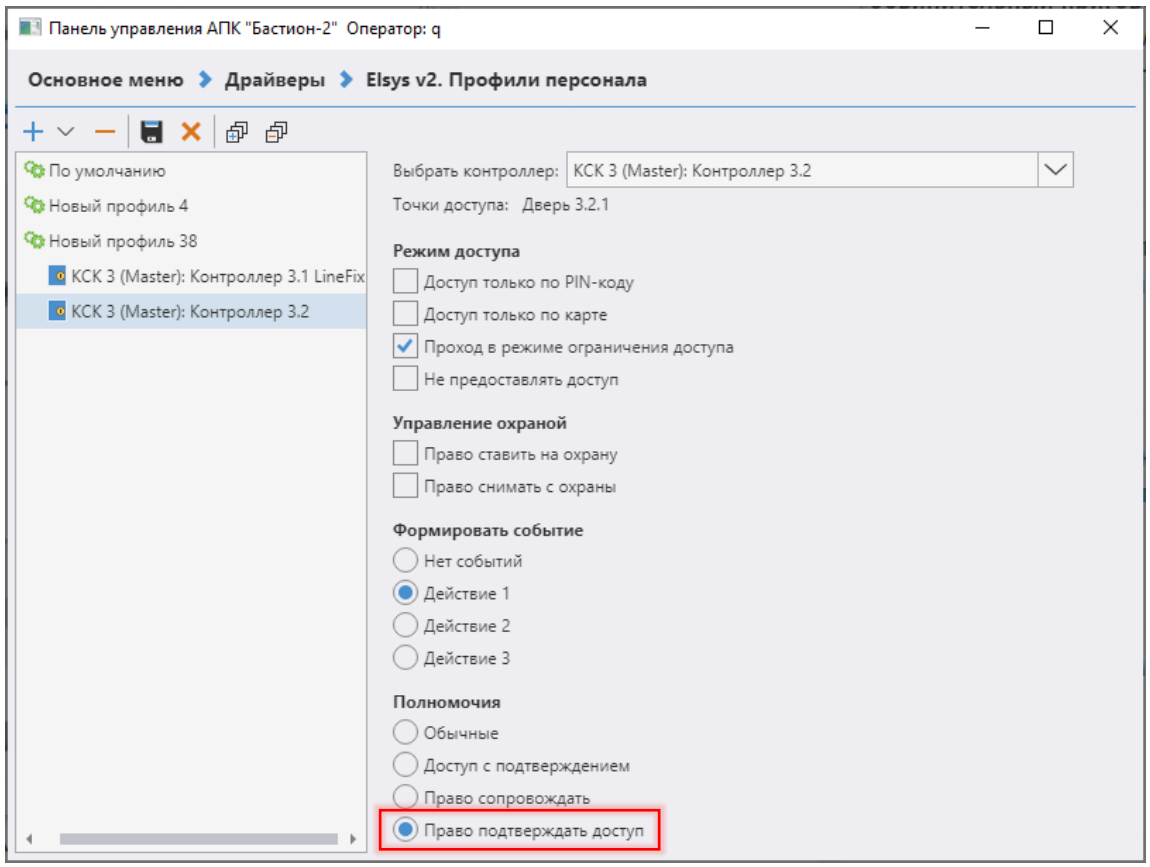


Рис. 30. Профиль настроек персонала для лиц, имеющих право подтверждать доступ

Для обеспечения работоспособности режима «доступ с подтверждением картой» необходимо убедиться, что на считывателе, где используется этот режим, отключены все полномочия дежурного оператора (см. Рис. 31).

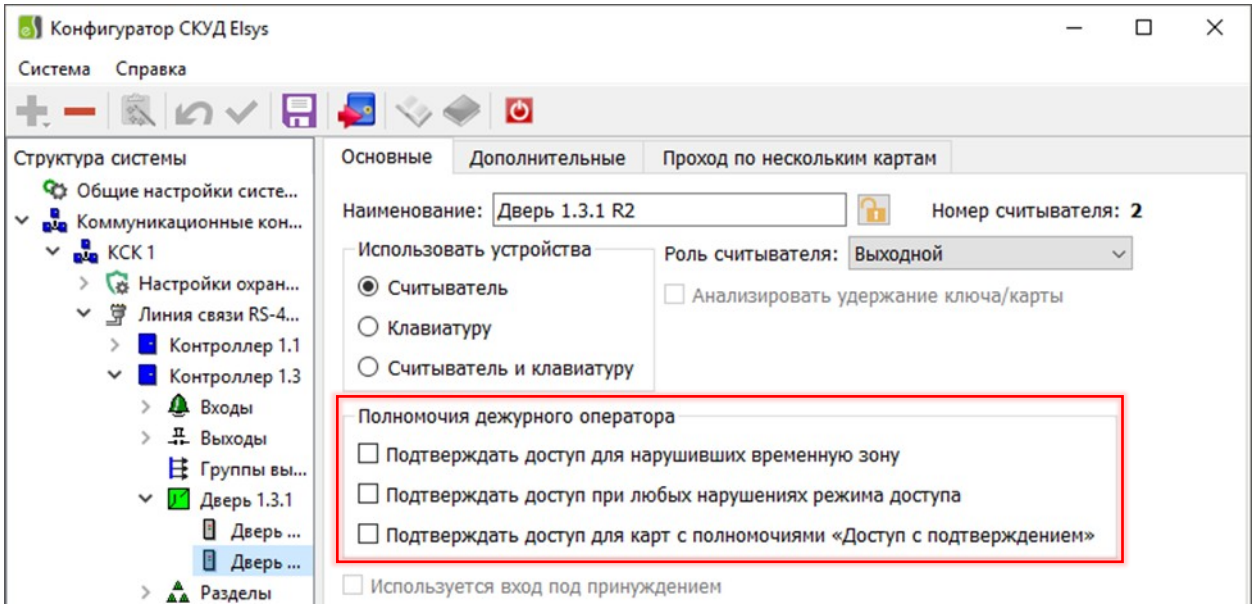


Рис. 31. Настройки считывателя, где используется режим «Доступ с подтверждением картой»

В противном случае контроллер после предъявления карты, требующей подтверждения, будет ожидать нажатия дежурным оператором кнопки подтверждения или отказа в доступе и не будет реагировать на подтверждающую карту.

На считывателях контроллера, где режим «Доступ с подтверждением» не нужен, необходимо включить настройку **«Игнорировать опцию пропуска «Доступ с подтверждением»** (см. Рис. 32).

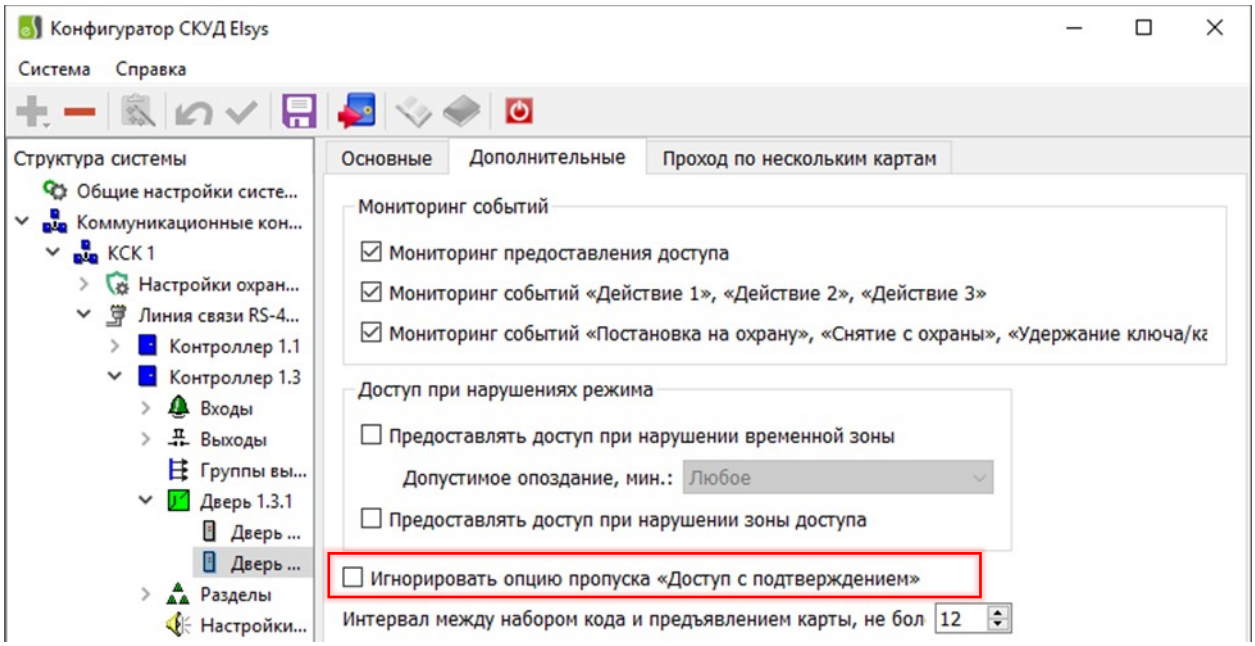


Рис. 32. Настройки считывателя, где необходимо выключить режимы «Доступ с подтверждением картой» и «Доступ с подтверждением кнопкой»

После предъявления карты, требующей подтверждения, индикатор считывателя сигнализирует мигающим зелёным светодиодом о том, что необходимо подтвердить доступ. Если в дополнение к световой индикации необходимо включить звуковую индикацию, необходимо настроить взаимодействия, как показано на Рис. 33.

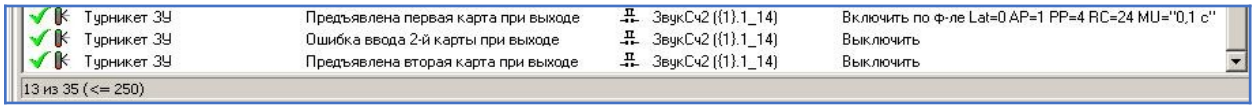


Рис. 33. Настройка звуковой индикации ожидания подтверждающей карты

3.9.4 Доступ с подтверждением оператором

Доступ с подтверждением оператором – встроенный усиленный алгоритм прохода, обеспечивающий для определённой категории пользователей СКУД (как правило, посетителей предприятия) доступ в отдельные точки прохода (находящиеся, как правило, на проходной предприятия) только с подтверждением дежурного оператора. На посту дежурного оператора должен быть установлен пульт с кнопками «Подтверждение доступа» и «Отказ в доступе» или модуль «Бастион 3 – Пост охраны».

На Рис. 34 показана последовательность регистрируемых событий при использовании доступа с подтверждением кнопкой (сценарием).

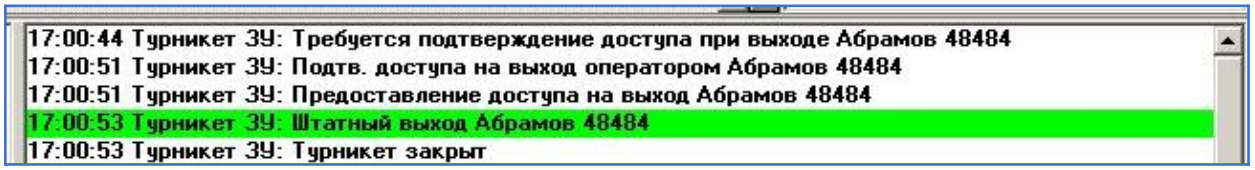


Рис. 34. Последовательность событий при использовании режима «Доступ с подтверждением кнопкой»

Для настройки режима «Доступ с подтверждением оператором» необходимо установить персональные настройки категориям лиц, которым требуется подтверждение доступа, включив опцию **«Доступ с подтверждением»**.

Для считывателя, где используется подтверждение доступа оператором, необходимо включить опции (см. Рис. 35):

- **«Вход для подтверждения доступа»** (вход контроллера, к которому подключена кнопка подтверждения доступа);
- **«Вход для отказа в доступе»** (вход контроллера, к которому подключена кнопка отказа в доступе);
- **«Подтверждать доступ для карт с полномочиями «Доступ с подтверждением»**.

После предъявления карты, требующей подтверждения, индикатор считывателя будет сигнализировать мигающим зелёным светодиодом о том, что необходимо подтвердить доступ. Если в дополнение к световой индикации необходимо включить звуковую индикацию, необходимо настроить взаимодействия, как показано на Рис. 36.

Оператор может подтверждать доступ, используя «Бастион-3 – Пост охраны», для чего необходимо создать соответствующий сценарий, указав в нём точку прохода и действие «Подтвердить доступ» или «Отказать в доступе». Более подробно настройка сценариев описана в документе «Бастион-3. Руководство администратора».

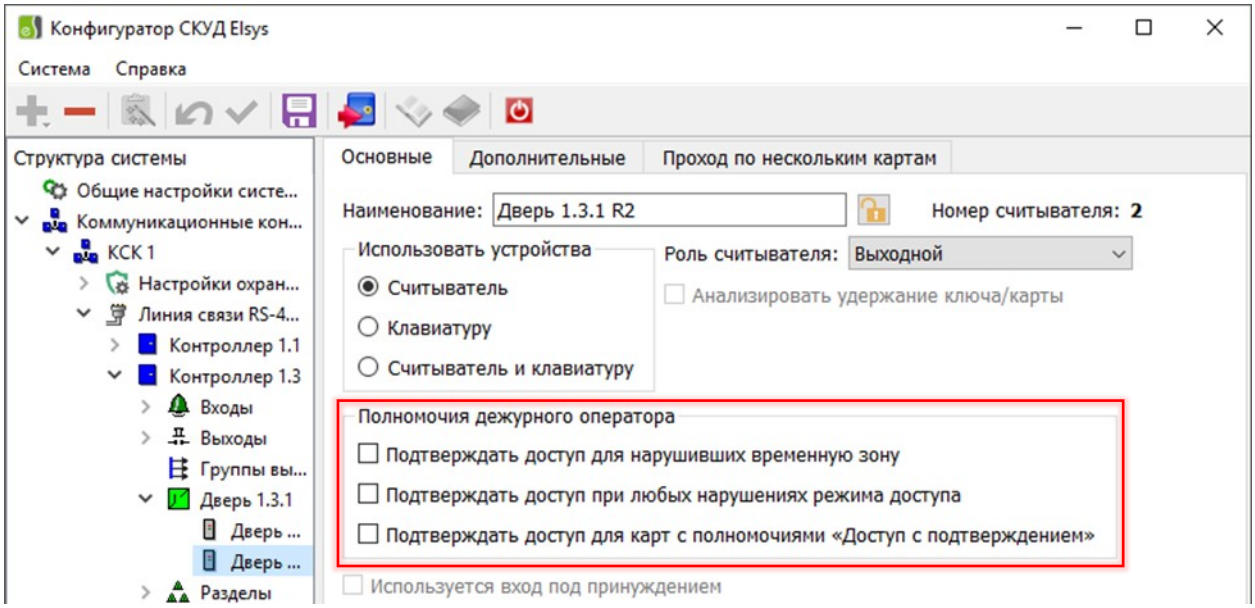


Рис. 35. Настройки считывателя, где используется режим «Доступ с подтверждением кнопкой»

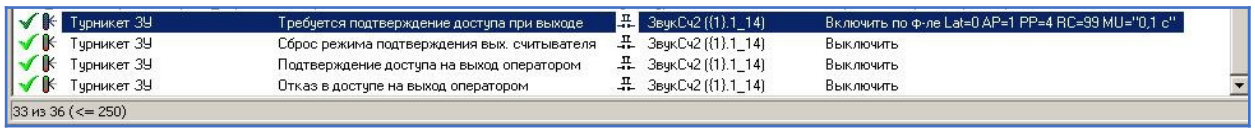


Рис. 36. Настройка звуковой индикации ожидания подтверждения оператора

4 Инициализация настроек персонала

Все изменения в базе данных пропусков (пропуска, уровни доступа, временные зоны, праздники) будут загружаться в контроллеры автоматически, при этом инициализация не требуется. В редких случаях при продолжительных потерях связи с отдельными контроллерами или в случае разрушительного сбоя их памяти может потребоваться ручная инициализация контроллеров.

Инициализация может быть выполнена с любого компьютера в сети ПК «Бастион-3» оператором, имеющим необходимые полномочия. В зависимости от полномочий оператора ряд опций инициализации может быть запрещён.

> ***Внимание!*** *Настройка и инициализация* ***оборудования*** *осуществляется при помощи автономного конфигуратора СКУД Elsys.*

Инициализация контроллеров вызывается с помощью кнопки **«Инициализация настроек персонала»,** расположенной на ленте управления драйвером (Рис. 2).

В окне инициализации (Рис. 37) отображаются все контроллеры СКУД Elsys с учётом с учетом привязки к Сетевым группам или КСК.

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

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

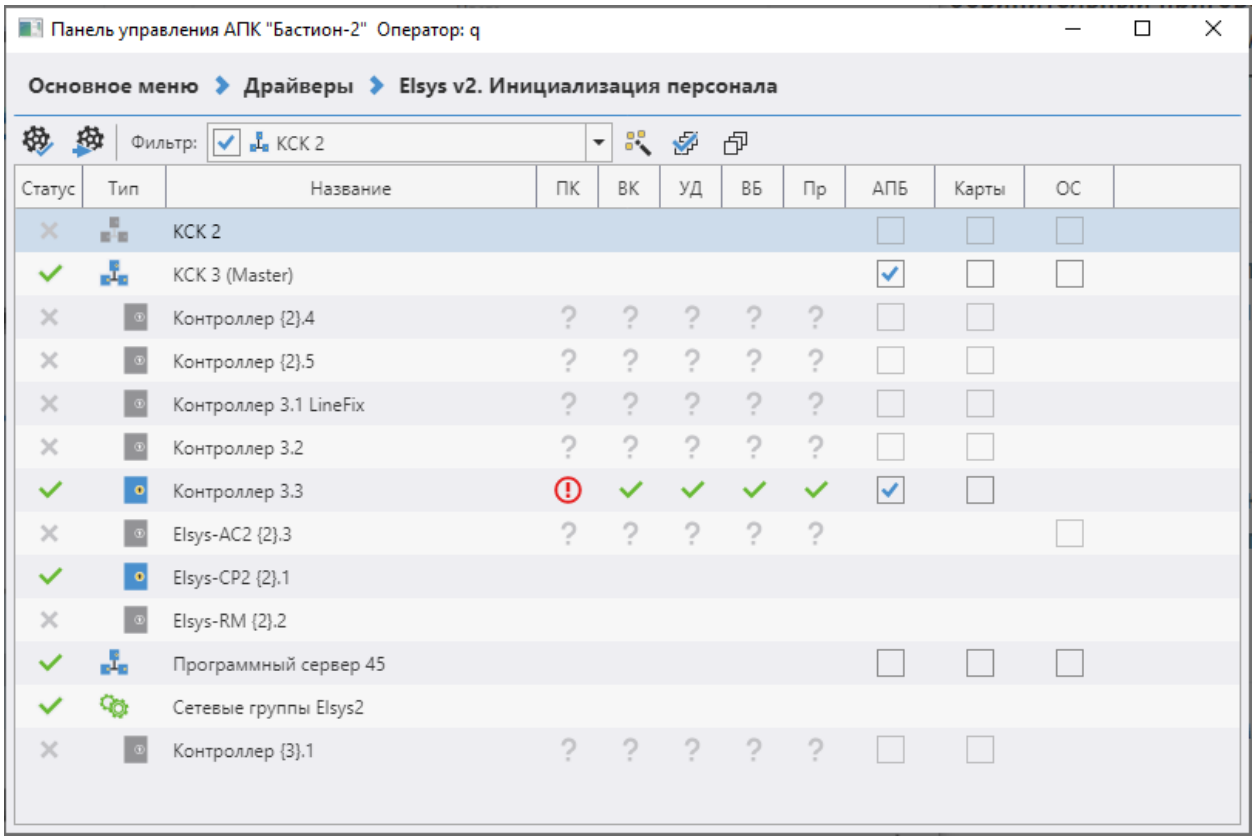


Рис. 37. Окно инициализации настроек персонала

По умолчанию отображаются все контроллеры системы. При их большом количестве можно перейти на требуемые КСК или Сетевую группу при помощи выпадающего списка. В этом же списке также можно отключить или включить отображение контроллеров, относящихся к той или иной Сетевой группе или КСК (Рис. 38).

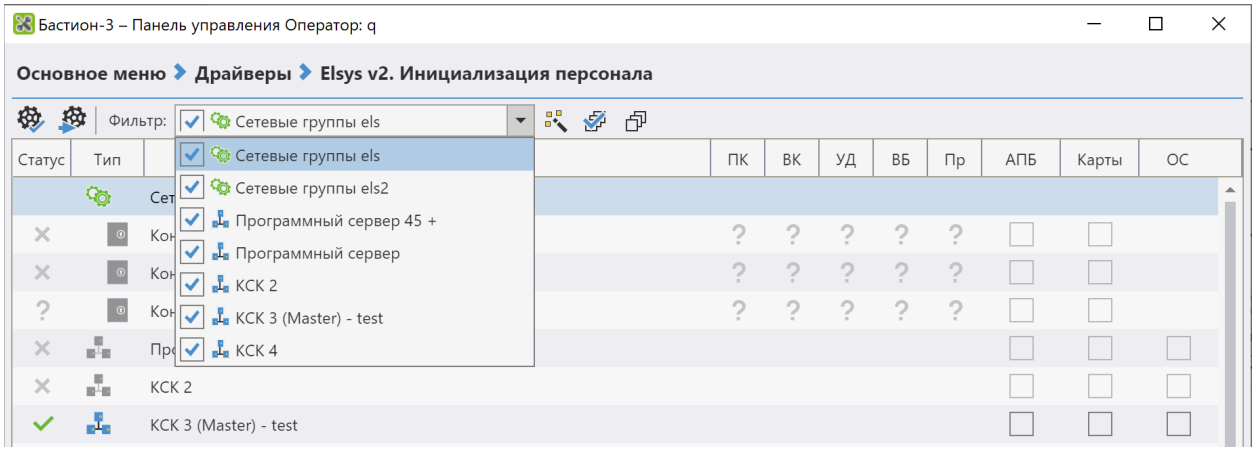
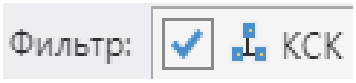


Рис. 38. Фильтрация и переход к КСК и сетевым группам

Назначение элементов на панели управления окна инициализации представлено в Табл. 5.

Табл. 5. Назначение элементов на панели управления окна инициализации

Элемент управления	Назначение
	Кнопка служит для запуска проверки конфигурации контроллеров. Проверка конфигурации запускается автоматически при открытии окна инициализации, а также после завершения инициализации. Результаты проверки конфигурации отображаются в виде пиктограмм (таблицы 3 и 4), а численные значения можно вывести в отдельном окне выбрав пункт контекстного меню **«Показать информацию».**
	Кнопка служит для запуска инициализации контроллеров, у которых установлены параметры инициализации.
	Выпадающий список всех КСК и сетевых групп, обеспечивающий быстрое перемещение по таблице контроллеров. Сняв или установив флаг напротив КСК или сетевой группы, можно скрыть или отобразить в таблице относящиеся к ним контроллеры.
	Кнопка служит для выделения всех контроллеров, имеющих проблемы с инициализацией
	Кнопка служит для выделения всех контроллеров на связи
	Кнопка служит для снятия выделения со всех контроллеров

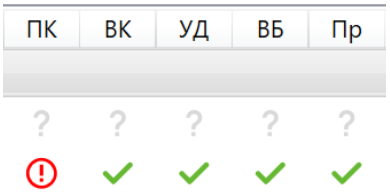
В первом столбце таблицы отображаются состояния контроллеров и сетевых групп. Описание возможных состояний представлено в Табл. 6.

Табл. 6. Описание возможных состояний контроллеров и сетевых групп

Пиктограмма	Описание состояния
(пусто)	Состояние контроллера неизвестно
	Контроллер на связи
	Потеря связи с контроллером
	Проблемы с инициализацией контроллера

Тип контроллера обозначается иконкой во втором столбце:

- Коммуникационный сетевой контроллер КСК.
- Сетевая группа.
- Контроллер СКУД или охранной подсистемы.



Третий столбец содержит названия контроллеров, присвоенные при конфигурировании.

В следующих 5 столбцах отображается состояние памяти контроллеров, получаемое при проверке конфигурации.

Описание столбцов представлено в Табл. 7, а описание возможных состояний представлено в Табл. 8.

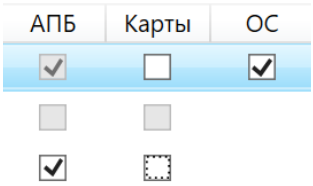
Табл. 7. Описание столбцов состояния памяти контроллеров

Пиктограмма	Описание состояния
ПК	Количество **П**остоянных **К**арт доступа
ВК	Количество **В**ременных и разовых **К**арт доступа
УД	Количество **У**ровней **Д**оступа
ВБ	Количество **В**ременных **Б**локов
Пр	Количество **Пр**аздничных дней

Табл. 8. Описание возможных состояний параметров памяти контроллеров

Пиктограмма	Описание состояния
	Состояние параметра не проверено или не определено
	Количество элементов в памяти контроллера соответствует количеству записей в базе данных
	Количество элементов в памяти контроллера **не** соответствует количеству записей в базе данных

Для каждого контроллера можно выбрать, что именно надо для него инициализировать:



«АПБ» – antipassback – инициализация параметров областей контроля для работы контроля последовательности прохода.

«Карты» – инициализация карт доступа с учетом профилей персонала.

«ОС» – инициализация карт управления охранной подсистемой.

Для удобства выбора параметров инициализации в контекстном меню доступно быстрое выделение определенных параметров группы контроллеров, относящихся к определенному КСК или сетевой группе (Рис. 39).

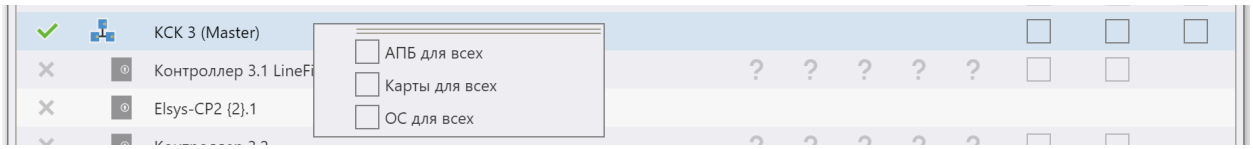


Рис. 39. Выбор типа инициализации для всех контроллеров группы

Из контекстного меню строки контроллера можно выполнить определенные команды для текущего контроллера (Рис. 40).

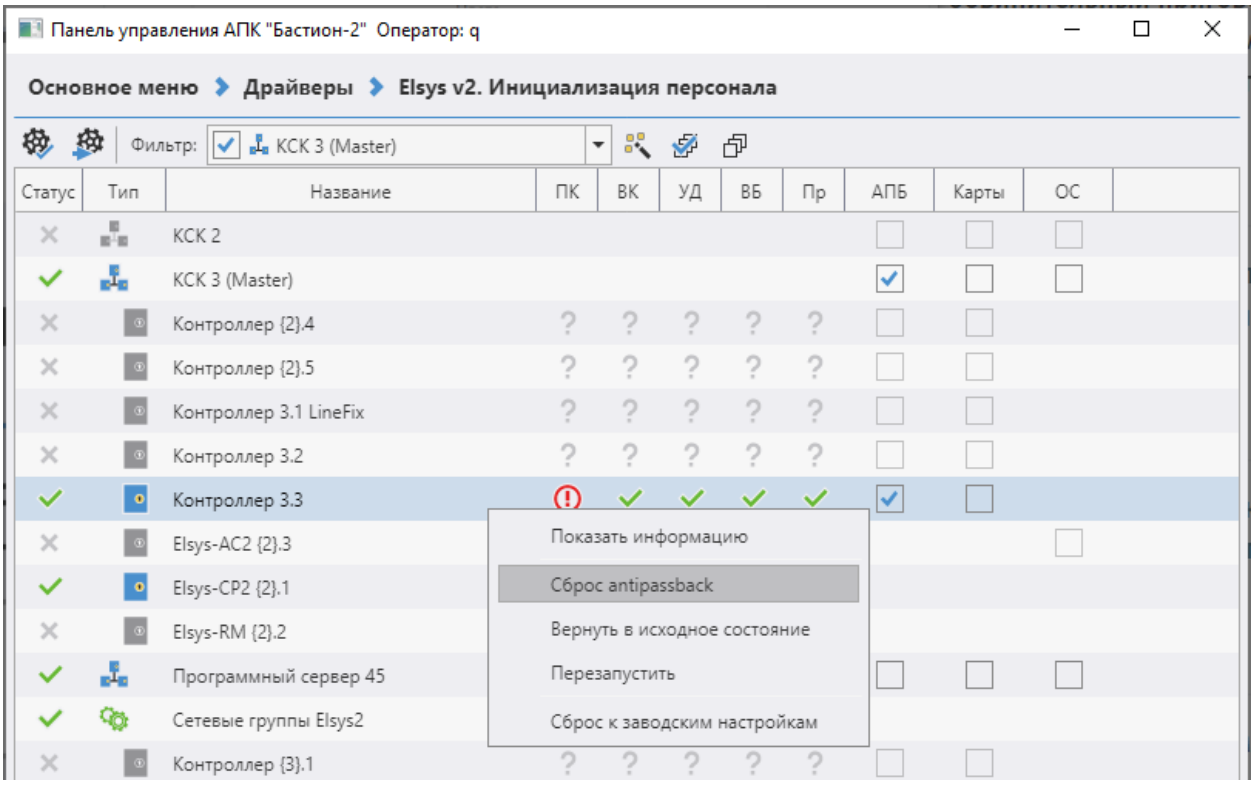


Рис. 40. Выбор всех типов инициализации для выбранного контроллера

Пункт меню **«Показать информацию»** откроет окно с подробным описанием численных параметров состояния памяти контроллера (Рис. 41).

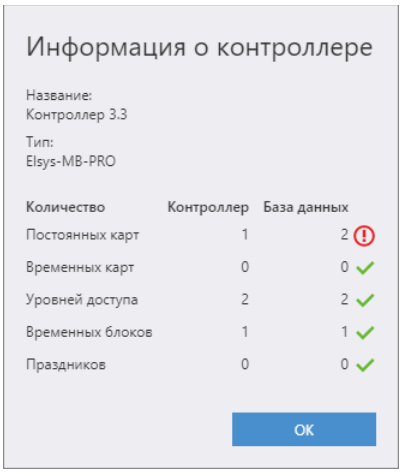


Рис. 41. Выбор всех типов инициализации для выбранного контроллера

Команда **«Сброс antipassback»** сбросит текущее местоположение пропусков для выбранного контроллера.

Команда **«Вернуть в исходное состояние»** переведет все устройства контроллера в состояние «по умолчанию» (выходы в состояние «выключены», входы в состояние «снято», двери в «нормальное состояние» и т. д.).

Команда **«Перезапустить»** выполнит перезапуск выбранного контроллера, аналогично нажатию на нем кнопки **Reset**.

Команда **«Сброс к заводским настройкам»** удалит из контроллера конфигурацию оборудования и вернет их настройки к заводским значениям.

> ***Внимание!*** *После сброса контроллера к заводским настройкам для его дальнейшей корректной работы потребуется его инициализация в «Автономном конфигураторе», обновление (при изменении конфигурации) дерева устройств, а также инициализация настроек персонала.*

Инициализацию следует проводить после начальной настройки системы и внесения изменений в настройку оборудования.

> ***Внимание!*** *Если в процессе настройки добавлялись контроллеры, добавлялись или удалялись двери, считыватели, турникеты, или изменялось распределение памяти контроллеров, необходимо полностью проинициализировать все контроллеры.*

Инициализацию антипассбэка следует проводить во всех контроллерах, если вносились изменения в конфигурацию областей контроля, а также при начальной настройке системы.

> ***Внимание!*** *Следует учитывать, что в процессе инициализации оборудование может работать неверно. Так, при инициализации списка карт доступа сначала полностью очищается список карт контроллера, а затем по одной заносятся новые карты. Соответственно, карты доступа, которые в текущий момент времени ещё не проинициализированы, будут опознаваться как «Неизвестная карта».*

5 Восстановление протокола событий

Для контроллеров доступа с версией прошивки 2.60 и выше существует возможность прочитать события из контроллера за указанный интервал времени (восстановить протокол событий), если произошел сбой базы данных с потерей информации (Рис. 42).

Внимание! *Восстановление протокола событий – длительная операция, которая приводит к большой загрузке системы и может на некоторое время нарушить ее нормальную работу.*

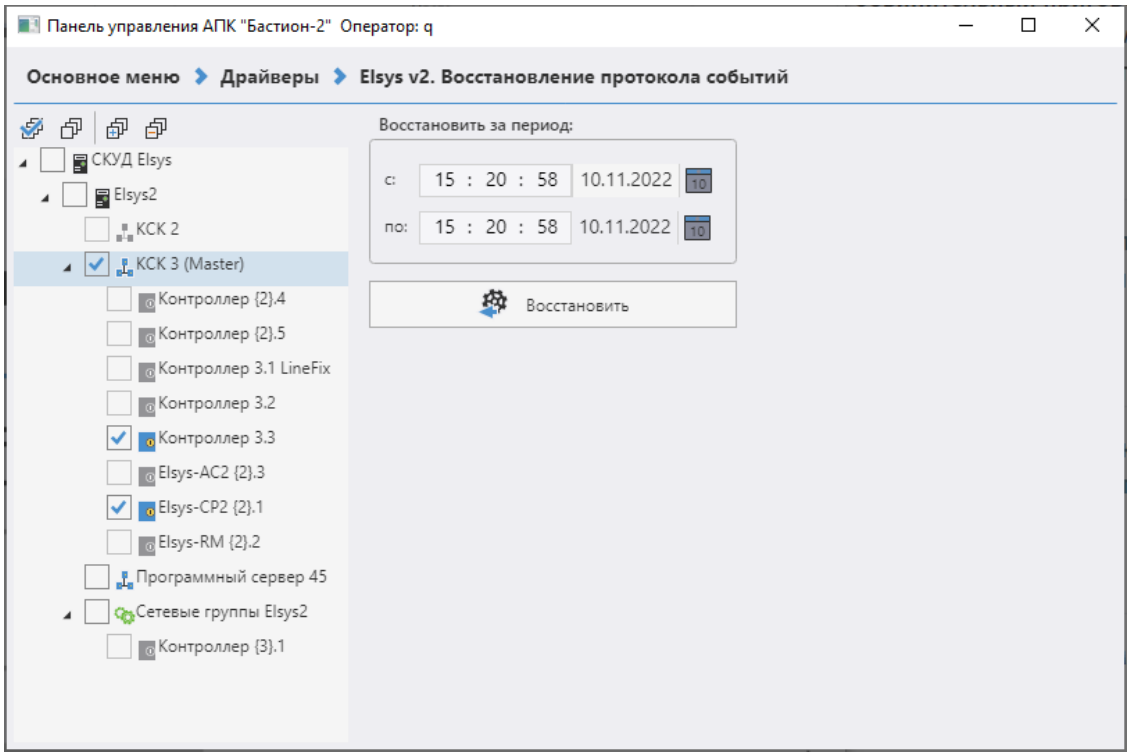


Рис. 42. Окно настройки восстановления протокола

Окно восстановления протокола событий запускается с помощью кнопки «**Восстановление протокола событий**», расположенной на ленте управления драйвера (Рис. 2).

Для восстановления протокола событий следует выбрать все контроллеры, события от которых следует восстановить, задать период времени и нажать кнопку «**Восстановить**».

При указании периода времени обязательным является задание начальной даты. Для задания даты и времени окончания периода следует установить опцию «**по**» и задать требуемые значения. Если указано только начало периода, то будут восстановлены все события с начала указанного периода времени.

При успешном восстановлении протокола событий будет сформировано событие контроллера «Восстановление буфера событий».

При частичном восстановлении протокола событий будет сформировано событие «Частичное восстановление буфера событий».

Внимание! *Для корректной работы функции восстановления протокола событий должны быть выполнены следующие условия:*

1) дата конца периода не должна превышать текущей даты (время может быть до 23:59 от текущей даты;

2) если текущий месяц находится в диапазоне с января по ноябрь, то допустимо указать месяц начала периода - декабрь, при этом будет считаться, что это предыдущий год;

3) если текущий месяц - декабрь, то месяц начала периода допустимо задавать в диапазоне с января по декабрь, при этом будет считаться, что это текущий год;

4) дата начала периода не должна превышать дату конца периода (кроме п. 2, где считается, что это предыдущий год).

Приложения

Приложение 1. События драйвера

В этом разделе приведены все события драйвера «Бастион-3 – Elsys». Большинство событий регистрируются в буфере событий контроллера (некоторые из них – опционально), затем передаются и обрабатываются компьютером. Ниже описано участие событий во взаимодействиях и в записи в буфер событий. Более подробная информация о событиях приведена в «Руководстве по эксплуатации СКУД Elsys».

События выходов и групп выходов

События выходов перечислены в Табл. 9.

Табл. 9. События выходов и групп выходов

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Включение	Да	Да	События пишутся в буфер только при включенной опции «Мониторинг состояния выхода»
Выключение	Да	Да	
Окончание работы по формуле	Да	Да	Событие пишется в буфер только при включенной опции «Мониторинг окончания работы по формуле»

События выходов «Включение» и «Выключение» регистрируются в момент изменения состояния выхода, а событие «Окончание работы по формуле» - в момент окончания работы формулы (если работа выхода по формуле не была прервана командой «Включить» или «Выключить»). Взаимодействия на эти события обрабатываются всегда, независимо от того, включена их регистрация в буфере событий, или нет. Группы обладают всеми свойствами выхода и могут формировать те же события. Пустые группы можно использовать в разных вспомогательных целях.

События точек доступа

Самый обширный список событий – у точек доступа (дверей, турникетов и ворот/шлагбаумов). Эти события можно разделить на три группы. Первая группа – события, фактически повторяющие события датчика прохода («Взлом», «Открытие двери», «Удержание двери» и т. д.), при этом соответствующие события датчика прохода не регистрируются в протоколе (однако, возможно назначение на них аппаратных взаимодействий). События этой группы приведены в Табл. 10.

Последние четыре события формируются драйвером «Бастион-3 – Elsys» вместо сообщаемых контроллером событий «Штатный вход» и «Штатный выход», если им предшествовала одна из описанных ниже последовательностей событий: «Нарушение временной зоны» («Нарушение зоны доступа») и «Предоставление доступа» с одинаковым временем (с точностью до секунды).

Табл. 10. События, формируемые при срабатывании датчика прохода

Событие	Участие во взаимодей-ствиях	Запись в буфер событий	Комментарий
Штатный вход (+ № карты)	Да	Да	
Штатный выход (+ № карты)	Да	Да	
Вход под принуждением (+ № карты)	Да	Да	
Выход под принуждением (+ № карты)	Да	Да	
Дверь не заперта	Да	Да	Только для дверей с электромеханическим замком
Взлом	Да	Да	
Удержание	Да	Да	
Закрытие двери	Да	Да	
Открывание двери	Да	Да	Используется для мониторинга состояния дверного контакта при разблокированной двери
КЗ дверного контакта	Да	Да	При обработке взаимодействий – событие «Неисправность»
Обрыв дверного контакта	Да	Да	При обработке взаимодействий – событие «Неисправность»
Фактический выход по кнопке	Нет	Да	
Ворота закрыты	Да	Да	Только для ворот
Ворота приоткрыты	Да	Да	Только для ворот
Ворота открыты полностью	Да	Да	Только для ворот

Событие	Участие во взаимодей-ствиях	Запись в буфер событий	Комментарий
Вход с нарушением временной зоны (+ № карты)	Нет	Нет	Формируется драйвером на основе предыстории событий вместо сообщаемого контроллером события «Штатный вход»
Выход с нарушением временной зоны (+ № карты)	Нет	Нет	Формируется драйвером на основе предыстории событий вместо сообщаемого контроллером события «Штатный выход»
Вход с нарушением зоны доступа (+ № карты)	Нет	Нет	Формируется драйвером на основе предыстории событий вместо сообщаемого контроллером события «Штатный вход»
Выход с нарушением зоны доступа (+ № карты)	Нет	Нет	Формируется драйвером на основе предыстории событий вместо сообщаемого контроллером события «Штатный выход»

Такая последовательность может быть сформирована лишь в случае, если используется «мягкий» режим доступа (т. е. для считывателей включена одна из опций «Предоставлять доступ при нарушении временной зоны» или «Предоставлять доступ при нарушении зоны доступа»). Для считывателя обязательно должна быть включена опция «Мониторинг предоставления доступа» (в противном случае событие «Предоставление доступа» не будет сформировано).

«Нарушение временной зоны» («Нарушение зоны доступа»), «Подтверждение доступа оператором», «Предоставление доступа» (последнее событие может отсутствовать, если выключена опция «Мониторинг предоставления доступа»). Такая последовательность может быть сформирована, если используются контроллеры версий 1.37 (т. к. начиная с этой версии регистрируется событие «Подтверждение доступа оператором») и выше, а также используется режим с подтверждением доступа оператором.

Описанные выше события «Вход/Выход с нарушением…» могут быть использованы при формировании отчётов о нарушителях режима доступа.

Вторая группа, самая многочисленная, – это события, связанные с предъявлением карты (большинство подобных событий имеются в двух вариантах – для входного и для выходного считывателя; полный текст этих событий содержит информацию о том, на каком считывателе, входном или выходном, произошло событие). Все эти события также содержат также номер карты или PIN-код. События этой группы приведены в Табл. 11.

Табл. 11. События точек доступа, связанные с предъявлением карты доступа

Событие	Участие во взаимодей-ствиях	Запись в буфер событий	Комментарий
Предоставление доступа	Да	Да	События записываются в буфер только при включенной опции «Мониторинг предоставления доступа»
Предоставление доступа под принуждением	Да	Да	
Нарушение зоны доступа	Да	Да	
Отказ в доступе - нет прав	Да	Да	
Нарушение временной зоны	Да	Да	
Неизвестная карта	Да	Да	
Неизвестный PIN-код	Да	Да	
Запрет доступа (ограничение доступа)	Да	Да	
Отказ в доступе – блокировка	Да	Да	
Неверный PIN-код	Да	Да	
Отказ в доступе - нет полномочий	Да	Да	
Ошибка ввода второй карты	Да	Да	
Ошибка ввода третьей карты	Да	Да	
Любое нештатное событие	Да	Нет	
Предъявлена первая карта	Да	Нет	

Событие	Участие во взаимодей-ствиях	Запись в буфер событий	Комментарий
Предъявлена вторая карта	Да	Нет	
Предъявлена третья карта	Да	Нет	
Действие 1	Да	Да	События записываются в буфер только при включенной опции «Мониторинг пользовательских безусловных действий»
Действие 2	Да	Да	
Действие 3	Да	Да	
Постановка на охрану	Да	Да	События записываются в буфер только при включенной опции «Мониторинг пользовательских условных действий». Событие записывается к кодом карты.
Снятие с охраны	Да	Да	
Требуется подтверждение доступа	Да	Да	События записываются в буфер только при включенной опции «Мониторинг предоставления доступа»
Подтверждение доступа оператором	Да	Да	В буфер событий записывается событие «Штатное предоставление доступа». Начиная с версии 1.37 контроллеры регистрируют также событие «Подтверждение доступа оператором»
Отказ в доступе оператором	Да	Да	
Подтверждение доступа картой	Нет	Да	
Сброс режима подтверждения	Да	Нет	
Ввод пароля (входной считыватель)	Да	Нет	Ввод одного из 16 служебных PIN-кодов
Ввод пароля (выходной считыватель)	Да	Нет	Ввод одного из 16 служебных PIN-кодов

Событие	Участие во взаимодей-ствиях	Запись в буфер событий	Комментарий
Ввод пароля и предъявление карты (входной считыватель)	Да	Нет	
Ввод пароля и предъявление карты (выходной считыватель)	Да	Нет	
Штатное предъявление служебной карты (входной считыватель)	Да	Нет	
Штатное предъявление служебной карты (выходной считыватель)	Да	Нет	
Предъявление служебной карты (входной считыватель)	Да	Да	16 событий, соответствующих отдельным действиям при вводе служебного PIN-кода и предъявлении карты
Предъявление служебной карты (выходной считыватель)	Да	Да	16 событий, соответствующих отдельным действиям при вводе служебного PIN-кода и предъявлении карты

И, наконец, третья группа – это события-команды для турникетов и ворот, используемые для задания специфичных для разных типов устройств алгоритмов. Список этих событий приведён в приведённых ниже Табл. 12, Табл. 13.

Табл. 12. События-команды для ворот

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Открыть	Да	Нет	
Закрыть	Да	Нет	
Стоп	Да	Нет	
Заблокировать	Да	Нет	

Табл. 13. События-команды для турникета

Событие	Участие во взаимодей-ствиях	Запись в буфер событий	Комментарий
Заблокировать вход	Да	Нет	
Заблокировать выход	Да	Нет	
Разблокировать вход	Да	Нет	
Разблокировать выход	Да	Нет	
Нормальный режим (вход)	Да	Нет	
Нормальный режим (выход)	Да	Нет	

События входов

События, регистрируемые на входах контроллеров Elsys-MB, приведены в Табл. 14. Любой вход имеет четыре основных состояния («на охране», «норма – готов к постановке на охрану»; «тревога»/ «неготовность шлейфа»). Соответственно, это две пары физических состояний цифрового входа, соответствующие режимам «На охране» и «Вне охраны». Опция **«Фиксировать тревогу»** должна быть включена, если предполагается использовать вход как охранный. В этом режиме тревожное состояние входа сохраняется до тех пор, пока не придёт команда («постановка на охрану» или «снятие с охраны»).

Табл. 14. События входов

Событие	Участие во взаимо-действиях	Запись в буфер событий	Комментарий
Обрыв	Да	Да	Событие пишется в буфер только при включенной опции **«Мониторинг состояния входа»**. При обработке взаимодействий события «Обрыв» и «Короткое замыкание» интерпретируются как неисправность
Короткое замыкание	Да	Да	
Норма (готов к взятию на охрану)	Да	Да	События пишутся в буфер только при включенной опции **«Мониторинг состояния входа»**
Неготовность шлейфа	Да	Да	

Событие	Участие во взаимо-действиях	Запись в буфер событий	Комментарий
На охране	Да	Да	
Тревога	Да	Да	
Удержание	Да	Да	
Невзятие на охрану	Да	Да	
Снятие с охраны	Да	Да	
Задержка взятия	Да	Да	
Задержка взятия - неготовность	Да	Да	
Задержка тревоги	Да	Да	
Неисправность	Да	Да	

Если опция **«Фиксировать тревогу»** выключена, состояние входа регистрируется в зависимости от того, на охране он или нет. Опция «Отслеживать состояние вне охраны» может быть выключена, если события о готовности/неготовности входа к постановке на охрану неинтересны и засоряют протокол (например, открытие/закрытие двери торгового центра в часы работы; то же, в ночные часы, если зона на охране – является тревогой). Если зона не готова к постановке на охрану, а производится попытка поставить вход на охрану, формируется событие «Не взятие».

События контроллеров

События, относящиеся к устройству «Контроллер», приведены в Табл. 15.

Табл. 15. События контроллеров

Событие	Участие во взаимо-действиях	Запись в буфер событий	Комментарий
Выключение питания	Нет	Да	
Включение питания	Нет	Да	

Событие	Участие во взаимо-действиях	Запись в буфер событий	Комментарий
Очистка конфигурации	Нет	Да	
Разрушение БД контроллера	Нет	Да	
Сброс программный	Да	Да	
Сброс аппаратный	Нет	Да	
Авария первичного электропитания	Нет	Да	
Восстановление первичного электропитания	Нет	Да	
Взлом корпуса	Нет	Да	
Восстановление зоны контроля взлома	Нет	Да	
Потеря связи	Нет	Нет	События формируются драйвером «Бастион-3 – Elsys»
Восстановление связи	Нет	Нет	
Сброс антипассбэка	Нет	Нет	
Инициализация	Нет	Нет	
Ошибка в процессе инициализации	Нет	Нет	
Аккумулятор в норме	Нет	Да	
Аккумулятор разряжен	Нет	Да	
Включение режима MASTER-SLAVE	Нет	Да	
Включение режима MULTIMASTER	Нет	Да	
Включение режима UDP	Нет	Да	
Выключение режима UDP	Нет	Да	
Восстановление буфера событий	Нет	Да	
Частичное восстановление буфера событий	Нет	Да	
Восстановление связи между Elsys-MB и Elsys-IP	Нет	Да	
Нет связи между Elsys-MB и Elsys-IP	Нет	Да	
Отсутствует модуль расширения памяти	Нет	Да	

Событие	Участие во взаимо-действиях	Запись в буфер событий	Комментарий
Некорректный номер временного блока	Нет	Нет	События формируются драйвером «Бастион-3 – Elsys»
Некорректный номер уровня доступа	Нет	Нет	
Превышено допустимое количество временных зон	Нет	Нет	
Превышено допустимое количество постоянных карт	Нет	Нет	
Превышено допустимое количество уровней доступа	Нет	Нет	
Срабатывание сторожевого таймера	Нет	Да	

На событие «Сброс» (взаимодействия на него обрабатываются в момент сброса или включения питания) может быть назначен ряд действий, приводящих в исходное состояние все устройства (выходы – включить, входы – взять под охрану, двери – вернуть в нормальный режим и т. п.).

Сообщение о потере связи с контроллером генерируется компьютером в том случае, если несколько раз подряд контроллер не передавал очередных сообщений.

Сообщение о восстановлении связи генерируется в следующих случаях:

а) установка связи с одним из контроллеров, занесенных в базу данных драйвера;

б) запуск программы;

в) вход в программу под другим именем.

Кроме того, сообщения о потере и восстановлении связи генерируются при выходе из конфигуратора оборудования. Это связано с тем, что в этот момент драйвер временно приостанавливает обмен с контроллерами и перечитывает конфигурацию оборудования из базы данных.

Ряд событий, используемых при настройке взаимодействий, и формально относящихся также к устройству «Контроллер», описаны в Табл. 16.

Табл. 16. Дополнительные события

Событие	Участие во взаимодейс твиях	Запись в буфер событий	Комментарий
Начало временного блока	Да	Нет	Доп. параметр - № врем. блока (1...125)

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Окончание временного блока	Да	Нет	Доп. параметр - № врем. блока (1...125)
Активность логической формулы	Да	Нет	Доп. параметр - № логической формулы (1...20)
Неактивность логической формулы	Да	Нет	Доп. параметр - № логической формулы (1...20)
Восстановление связи с другим контроллером	Да	Нет	Доп. параметр – адрес контроллера (0 – компьютер, 64 – все контроллеры)
Потеря связи с другим контроллером	Да	Нет	Доп. параметр – адрес контроллера (0 – компьютер, 64 – все контроллеры)
Сообщение от контроллера	Да	Нет	Доп. параметры – адрес контроллера (64 – любой контроллер) и № сообщения (1...64)
Счётчик (POSTDEC) равен значению	Да	Нет	Доп. параметры - № счётчика (1...8) и значение (0...63)
Счётчик (POSTINC) равен значению	Да	Нет	Доп. параметры - № счётчика (1...8) и значение (0...63)
Счётчик равен значению	Да	Нет	Доп. параметры - № счётчика (1...8) и значение (0...63)

События разделов

События разделов приведены в Табл. 17.

Табл. 17. События разделов

Событие	Участие во взаимодействиях	Запись в буфер событий	Комментарий
Взятие на охрану	Да	Да	События пишутся в буфер только при включенной опции в свойствах раздела **«Протоколировать события»**
Взятие на охрану с задержкой	Да	Да	
Невзятие на охрану	Да	Да	
Снятие с охраны	Да	Да	

Тревога	Да	Да	
Тревога входной зоны	Да	Да	

События сетевых контроллеров Elsys-MB-Net

События, формируемые сетевыми контроллерами Elsys-MB-Net, приведены в Табл. 18.

Табл. 18. События, формируемые контроллерами Elsys-MB-Net

Событие	Комментарий
Включение режима MULTIMASTER	Формируется КСК Elsys-MB-Net в момент включения режима «MULTIMASTER»
Включение режима MASTER-SLAVE	Формируется КСК Elsys-MB-Net в момент включения режима «MASTER-SLAVE»
Срабатывание сторожевого таймера	Формируется в случае сброса КСК Elsys-MB-Net по сторожевому таймеру
Сброс программный	Формируется в случае сброса КСК Elsys-MB-Net по внешней команде
Сброс аппаратный	Формируется в случае сброса КСК Elsys-MB-Net кнопкой RESET
Разрушение БД контроллера	Формируется в случае обнаружения сетевым контроллером ошибок во внутренней базе данных. Необходимо выяснить, почему это произошло, и проинициализировать такой контроллер.
Потеря связи	Формируется драйвером в случае разрыва IP-соединения с КСК Elsys-MB-Net
Восстановление связи	Формируется драйвером в случае восстановления IP-соединения с КСК Elsys-MB-Net
Включение питания	Формируется КСК Elsys-MB-Net в момент включения сетевого питания
Выключение питания	Формируется КСК Elsys-MB-Net в момент выключения сетевого питания
Включение режима UDP	Формируется КСК Elsys-MB-Net в момент включения режима UDP
Выключение режима UDP	Формируется КСК Elsys-MB-Net в момент выключения режима UDP
Инициализация контроллера	Формируется драйвером в момент старта

Событие	Комментарий
	инициализации
Ошибка в процессе инициализации	Формируется драйвером при наличии ошибок инициализации

Приложение 2. Команды контроллеров Elsys-MB

В Табл. 19 приведены все команды, которые можно выполнить (сообщить контроллерам по интерфейсу RS-485), во-первых, из контекстных меню или вкладки «Управление» конфигуратора оборудования, а, во-вторых, с помощью предварительно настроенных аппаратных взаимодействий.

Табл. 19. Команды контроллеров Elsys-MB

Устройство	Команда	Диапазон значений аргументов
Вход	Поставить на охрану	0
	Поставить на охрану с задержкой	Интервал времени: 1..127 с
	Снять с охраны	0
	Снять с охраны на интервал времени	Интервал времени: 1..127 с
Выход	Включить	
	Выключить	
	Переключить состояние на противоположное	
	Включить по формуле	Номер формулы: 0..15
Дверь	Открыть	
	Заблокировать	
	Нормальный режим	
	Разблокировать	
Считыватель	Заблокировать	0
	Заблокировать на интервал времени	Интервал времени: 1...63 с
	Снять блокировку	0
	Снять блокировку на интервал времени	Интервал времени: 1...63 с
	Ограничить доступ	
	Снять ограничение доступа	

Устройство	Команда	Диапазон значений аргументов
Турникет	Открыть на вход	
	Заблокировать на вход	
	Нормальный режим (вход)	
	Разблокировать на вход	
	Открыть на выход	
	Заблокировать на выход	
	Нормальный режим (выход)	
	Разблокировать на выход	
Ворота	Открыть	
	Закрыть	
	Стоп	
	Заблокировать	
	Нормальный режим	
Контроллер	Сформировать сообщение всем контроллерам	Адрес контроллера: 0, № сообщения: 1...64
	Сформировать сообщение контроллеру	Адрес контроллера: 1...63, № сообщения: 1...64
	Инкремент счётчика	№ счётчика: 1...8
	Декремент счётчика	№ счётчика: 1...8
	Установить значение счётчика	№ счётчика: 1...8, значение счетчика: 0...63
	Сбросить счётчик персонала	
	Сбросить счётчик персонала для УД	Номер УД: 1... 16382

Приложение 3. Индикация состояния на планах

Устройства, входящие в состав СКУД Elsys, могут быть представлены на графическом плане объекта в виде пиктограмм, многоугольников (охранные зоны), ломаных линий (периметр). Эти элементы отображают текущее состояние устройств, а также позволяют выполнять команды управления из контекстного меню.

Различным устройствам соответствует свой набор состояний пиктограмм. Состояния пиктограмм формируются драйвером «Бастион-3 – Elsys» на основе предыстории событий, действий оператора и других данных, сообщённых оборудованием.

Драйвер формирует состояние пиктограммы на основе неподтверждённых тревожных событий (к ним относятся сообщения о тревогах и неисправностях). В этом режиме, даже если тревожная ситуация прекратилась, вид пиктограммы будет определяться неподтверждённым тревожным событием. Если таких событий было несколько, вид пиктограммы выбирается в соответствии с наиболее приоритетным состоянием. Если все тревожные события подтверждены, состояние пиктограммы отображает реальное состояние устройства.

В таблицах ниже приведён набор состояний пиктограмм и их вид для устройств драйвера «Бастион-3 – Elsys». Значком  обозначены пиктограммы, которые находятся в мигающем режиме.

Табл. 20. Состояния устройств «контроллер», «КСК»

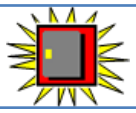
Состояние	Вид пиктограммы контроллера	Вид пиктограммы КСК	Описание	Приоритет тревожного состояния
Норма			Устройство исправно	
Неисправность			Отсутствие связи или неисправность (например: авария сетевого питания, разряд аккумулятора)	1
Тревога			Взлом корпуса	2

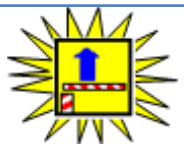
Табл. 21. Состояния дверей

Состояние	Вид пиктограммы	Описание	Приоритет тревожного состояния
Норма		Дверь закрыта	

Состояние	Вид пиктограммы	Описание	Приоритет тревожного состояния
Заблокировано		Дверь заблокирована. Доступ по предъявлению карты запрещён	
Разблокировано, дверь закрыта		Дверь разблокирована, находится в закрытом состоянии (датчик прохода замкнут)	
Разблокировано, дверь открыта		Дверь разблокирована, находится в открытом состоянии (датчик прохода разомкнут)	
Осуществление входа		Дверь в открытом состоянии. Состояние регистрируется после события «Штатный вход»	
Осуществление выхода		Дверь в открытом состоянии. Состояние регистрируется после события «Штатный выход»	
Дверь открыта		Дверь в открытом состоянии после выполнения команды «Открыть» и в иных случаях, когда направление прохода определить невозможно.	
Доступ разрешён, дверь закрыта		Дверь отперта, но находится в закрытом состоянии (датчик прохода замкнут). Состояние регистрируется после предоставление доступа по карте или выполнения команды «Открыть»	
Попытка нештатного входа		Было зарегистрировано нештатное предъявление карты при входе	1
Попытка нештатного выхода		Было зарегистрировано нештатное предъявление карты при выходе	2
Удержание двери		Дверь открыта, а время, отводимое на проход, истекло	3
Дверь не заперта		Дверь отперта, так как не был совершён проход. Состояние возможно только для дверей с электромеханическими замками-защёлками	4

Состояние	Вид пиктограммы	Описание	Приоритет тревожного состояния
Вход под принуждением		Было зарегистрировано событие «Предоставление доступа на вход под принуждением»	5
Выход под принуждением		Было зарегистрировано событие «Предоставление доступа на выход под принуждением»	6
Взлом		Дверь была открыта нештатным образом	7
Примечание – состояния, выделенные курсивом, формируются, только если включен режим **«Подтверждение тревог оператором»**			

Табл. 22. Состояния ворот (шлагбаумов)

Состояние	Вид пиктограммы для ворот	Вид пиктограммы для шлагбаума	Описание	Приоритет тревожного состояния
Норма			Закрыто	
Заблокировано			Ворота заблокированы. Доступ по предъявлению карты запрещён	
Полуоткрыто			Ворота частично открыты. Состояние регистрируется в процессе штатного открывания ворот. Для регистрации состояния необходимо наличие датчика закрытого состояния и датчика открытого состояния.	
Открыто			Ворота полностью открыты. Состояние регистрируется после штатного открывания ворот	
Попытка нештатного входа			Было зарегистрировано нештатное предъявление карты при входе	1

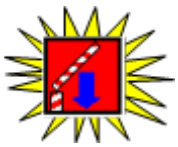
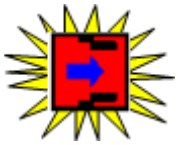
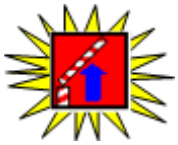
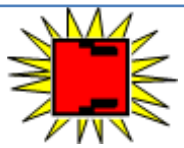
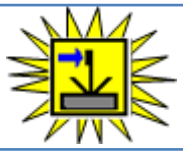
Состояние	Вид пиктограммы для ворот	Вид пиктограммы для шлагбаума	Описание	Приоритет тревожного состояния
Попытка нештатного выхода			Было зарегистрировано нештатное предъявление карты при выходе	2
Вход под принуждением			Было зарегистрировано событие «Предоставление доступа на вход под принуждением»	5
Выход под принуждением			Было зарегистрировано событие «Предоставление доступа на выход под принуждением»	6
Взлом			Ворота были открыты нештатным образом	7
Примечание – состояния, выделенные курсивом, формируются, только если включен режим **«Подтверждение тревог оператором»**				

Табл. 23. Состояния турникетов

Состояние	Вид пиктограммы	Описание	Приоритет тревожного состояния
Норма		Турникет закрыт (нормальный режим работы)	
Заблокировано		Турникет заблокирован на вход и на выход	
Разблокировано		Турникет разблокирован на вход и на выход	
Разблокировано на вход		Турникет разблокирован на вход, в направлении выхода работает в обычном режиме	
Разблокировано на выход		Турникет разблокирован на выход, в направлении входа работает в обычном режиме	
Заблокировано на вход		Турникет заблокирован на вход, в направлении выхода работает в обычном режиме	
Заблокировано на выход		Турникет заблокирован на выход, в направлении входа работает в обычном режиме	

Состояние	Вид пиктограммы	Описание	Приоритет тревожного состояния
Разблокировано на вход, заблокировано на выход		Турникет разблокирован на вход, заблокирован на выход	
Заблокировано на вход, разблокировано на выход		Турникет заблокирован на вход, разблокирован на выход	
Осуществление входа		Турникет в открытом состоянии. Состояние регистрируется после события «Штатный вход» или выполнения команды «Открыть на вход»	
Осуществление выхода		Турникет в открытом состоянии. Состояние регистрируется после события «Штатный выход» или выполнения команды «Открыть на выход»	
Осуществление прохода		Турникет в открытом состоянии (для случаев, когда направление прохода определить невозможно)	
Попытка нештатного входа		Было зарегистрировано нештатное предъявление карты при входе	1
Попытка нештатного выхода		Было зарегистрировано нештатное предъявление карты при выходе	2
Удержание		Датчик прохода в нарушенном состоянии, а время, отводимое на проход, истекло. Применительно к турникету это состояние означает, что поворотный механизм турникета удерживается в промежуточном положении	3

Состояние	Вид пиктограммы	Описание	Приоритет тревожного состояния
Вход под принуждением		Было зарегистрировано событие «Предоставление доступа на вход под принуждением»	5
Выход под принуждением		Было зарегистрировано событие «Предоставление доступа на выход под принуждением»	6
Взлом		Турникет был открыт нештатным образом	7
Примечание – состояния, выделенные курсивом, формируются, только если включен режим «Подтверждение тревог оператором»			

Табл. 24. Состояния выходов и групп выходов

Состояние	Вид пиктограммы	Описание
Включено		Управляющий выход включен
Выключено		Управляющий выход выключен

В Табл. 25 приведены списки возможных состояний для пиктограмм охранных зон (входов) и разделов. Для этих устройств не применяется программный механизм подтверждения тревог, так как тревожные состояния формируются на аппаратном уровне. Для сброса тревоги в охранной подсистеме необходимо выполнить для охранной зоны или для раздела команду снятия с охраны или постановки на охрану.

Табл. 25. Состояния входов и разделов

Состояние	Вид пиктограммы входа общего назначения	Вид пиктограммы охранного входа	Вид пиктограммы раздела	Описание
Снято с охраны				Состояние регистрируется, если вход или раздел снят с охраны и находится в состоянии «Норма – готовность к постановке

Состояние	Вид пиктограммы входа общего назначения	Вид пиктограммы охранного входа	Вид пиктограммы раздела	Описание
				на охрану»
На охране				Вход или раздел находится на охране или в состоянии «Задержка взятия - готовность»
Неготовность к постановке на охрану				Вход или раздел снят с охраны и находится в состоянии «Неготовность к постановке на охрану»
Тревога				Вход или раздел находятся в состоянии «Тревога» или «Задержка тревоги»
Неисправность				Состояние может быть зафиксировано только для тревожных входов, при регистрации короткого замыкания или обрыва
Примечание – Для охранных входов при настройке системы может быть задан иной вид пиктограмм и тип устройства				

Приложение 4. История изменений

2024.2 (06.09.2024)

[+] Поддерживается запуск конфигуратора Elsys из панели управления ПК «Бастион-3» с авторизацией операторов и разграничением прав доступа.

[+] Добавлена поддержка считывателей ESDP.

[+] Поддержаны проектные варианты исполнения контроллера NG-1000.

[*] Инициализация антипассбэка завершалась ошибкой. Исправлено.

[*] Запись логов перенесена в отладочную консоль.

[*] При смене уровня доступа у карты возникали ошибки конфигурации. Исправлено.

[*] Профили персонала могли иметь одинаковые имена. Исправлено.

[*] Не работали профили настроек персонала для контроллеров. Исправлено.

[*] Не восстанавливалась связь с сервисом интеграции после перезапуска драйвера. Исправлено.

[*] Исправлено ошибочное отображение состояния установки драйвера в «Мониторе состояний».

3.0.1 (10.11.2022)

Начальная версия модуля.