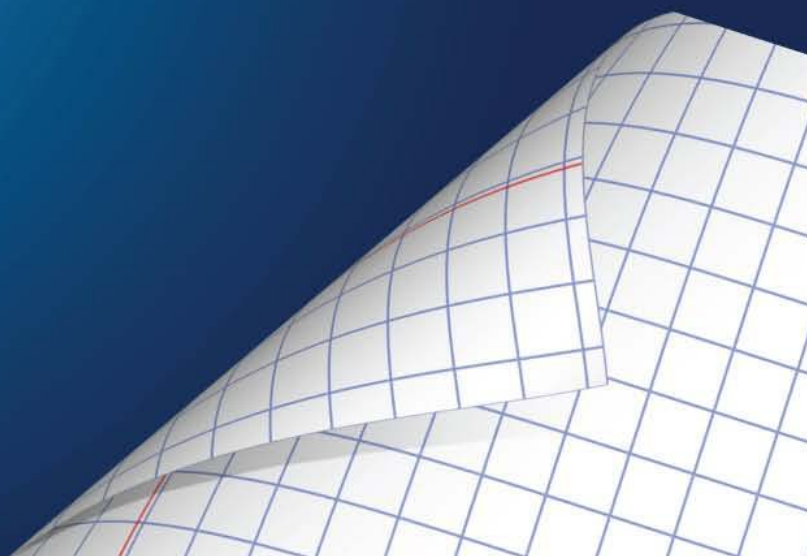


РУКОВОДСТВО АДМИНИСТРАТОРА

Программное обеспечение
PERCo-S-20 «Школа»



ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ	7
СОСТАВ СИСТЕМЫ PERCO-S-20 «ШКОЛА»	7
ПОРЯДОК ПОДГОТОВКИ СИСТЕМЫ К РАБОТЕ	9
ИНСТАЛЛЯЦИЯ ПО	9
Инсталляция PERCo-SS01 базовое ПО «Школа»	9
Удаление PERCo-SS01 базовое ПО «Школа»	11
ЛИЦЕНЗИИ	11
ОБЩИЕ СВЕДЕНИЯ	15
Настройка контроллера	19
Режим получения адреса	19
Настройка без DHCP	21
Настройка с DHCP	22
ОС Windows	22
ОС Linux	24
ОСОБЕННОСТИ РАБОТЫ СТЕКА ПРОТОКОЛА TCP/IP В WINDOWS XP SP1, SP2, SP3	26
КОНФИГУРАЦИЯ КОНТРОЛЛЕРОВ	26
Проведение конфигурации	27
Добавление нового устройства	29
Дополнительный вход	31
Дополнительный выход	34
Исполнительное устройство	38
Считыватель	39
Генератор тревоги	43
Шлейф сигнализации	45
Группы ресурсов	46
Защита от передачи идентификаторов	47

Протокол работы со считывателями	49
Описание параметров функционирования контроллеров КБО (серия CS01)	49
Контроллер.....	49
Дополнительный выход.....	50
Шлейф сигнализации	53
Зоны сигнализации	54
Исполнительное устройство	56
Считыватель	57
Генератор тревоги	61
Описание параметров функционирования контроллеров доступа (серия СТ/L04)	62
Дополнительный вход	62
Дополнительный выход.....	65
Шлейф сигнализации	68
Зоны.....	69
Исполнительное устройство	70
Считыватель	71
Генератор тревоги	75
Исключение из конфигурации.....	75
Удаление устройства	76
Удаленные устройства	77
Передача параметров устройства	77
Передача измененных параметров устройства	78
Добавление группы ресурсов	80
Изменение пароля	80
Изменение сетевых настроек	81
Получение информации о версиях прошивок	82
Изменение конфигурации контроллеров типа PERCo СТ/L04	82
Изменение параметров аппаратуры	83
Изменение протокола считывателей	85
Описание параметров видеоподсистемы.....	86

Видеоподсистема	86
Видеокамеры	87
НАЗНАЧЕНИЕ ПРАВ ДОСТУПА ОПЕРАТОРОВ	90
Добавление пользователя	91
Редактирование данных пользователя	92
Удаление пользователя	93
Предоставление прав доступа оператору	94
Права доступа на разделы	94
Права доступа на подразделения	95
Права доступа на помещения	96
Права доступа на управление устройствами	96
Запрет доступа пользователя	96
Копирование прав	96
УПРАВЛЕНИЕ СЕРВЕРАМИ	97
База данных	97
Созданные базы данных	99
Сохранение настроек базы данных	101
Сохранение базы данных	101
Восстановление базы данных из резервной копии	101
Удаление данных мониторинга	102
Удаление данных по событиям	102
Настройка сервера базы данных	102
Оптимизация индексов базы данных	104
Обновление версии базы данных	104
Восстановление предыдущего пароля устройств	104
Настройка работы с 1С	105
Проверка целостности БД	105
Резервное копирование БД	107
Настройка USB – Модема	111

Сервер видеонаблюдения	112
Сообщения об ошибках.....	113
ПОМЕЩЕНИЯ	114
Рабочее окно	115
Дерево помещений	115
Добавление внутреннего помещения	116
Добавление помещения на уровень выделенного помещения	117
Изменение названия помещения	118
Удаление помещения	120
Считыватели в дереве помещений	121
Печать.....	121
Экспорт в Excel	122
Изменение структуры дерева помещений.....	122
Доступные контроллеры	122
Устройства	125
Сортировка списков	126
ТРЕБОВАНИЯ К АППАРАТУРЕ	127
ПРИЛОЖЕНИЕ 1. СОБЫТИЯ	128
События, записываемые в журнал регистрации.....	128
События контроллера доступа (серия CL01, CL02, CL03, CT01, KT02).....	128
События, связанные с перемещением через ИУ	128
События, связанные с изменением текущего состояния дополнительных входов	130
События, связанные с изменением текущего состояния дополнительных выходов ...	131
События, связанные с изменением текущего состояния корпуса контроллера	131
События, связанные с работоспособностью сетевых каналов контроллера.....	131
События, связанные с изменением текущего состояния контроллеров или системы .	133
События, связанные с изменениями состояний группы ресурсов	135
События контроллеров КБО (серия CS01)	138

События, связанные с перемещением через ИУ	138
События, связанные с изменением текущего состояния дополнительных выходов ...	141
События, связанные с изменением текущего состояния корпуса контроллера	142
События, связанные с работоспособностью сетевых каналов контроллера.....	142
События, связанные с изменением текущего состояния контроллеров или системы .	144
События, связанные с изменениями состояний зон	146
События, связанные с изменением текущего состояния ШС, входящих в ОЗ и ПЗ.....	149
События, связанные с изменением текущего состояния ИУ, входящих в ОЗ	150
События контроллера доступа (серия СТ/L04)	151
События, связанные с перемещением через ИУ	151
События, связанные с изменением текущего состояния дополнительных входов	153
События, связанные с изменением текущего состояния дополнительных выходов ...	154
События, связанные с работоспособностью сетевых каналов контроллера.....	154
События, связанные с изменением текущего состояния контроллеров или системы .	156
События, связанные с изменением текущего состояния ШС, входящих в ОЗ	161
События, связанные с изменением текущего состояния ИУ, входящих в ОЗ	161
Команды управления.....	162
Контроллер управления доступом	162
Считыватель	164
Дополнительный выход	165
Группа ресурсов.....	165
Контроллер КБО	166
Зона контроллера КБО.....	168
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ	169

ВВЕДЕНИЕ

PERCo-S-20 "Школа" — это система безопасности с бесконтактными пластиковыми картами в качестве пропусков (далее — **система**), предназначенная для обеспечения безопасности школ, повышения контроля школьной дисциплины с возможностью оповещения родителей о времени прихода, ухода или прогула учеником школы с помощью SMS-сообщений и автоматизации учета посещаемости занятий.

Широкие возможности и надежность функционирования PERCo-S-20 «Школа» обеспечены рядом новых технических решений:

- Задачи обеспечения безопасности школ решаются с использованием одного и того же оборудования, линий связи, баз данных и программного обеспечения.
- Система совмещает функции системы охранной сигнализации, контроля и управления доступом, видеонаблюдения (расширенная версия).
- Все технические средства системы работают в единой информационной среде Ethernet, которая значительно упрощает и расширяет выбор IT-решений при монтаже.
- Реализована возможность оповещения родителей о времени прихода, ухода или неприхода учеником школы с помощью SMS-сообщений.
- Система дает возможность наращивания функций базового варианта и интеграции в существующие сети.

Программное обеспечение PERCo-S-20 «Школа» состоит из разделов, что позволяет формировать ПО под задачи конкретного заказчика.

Данное руководство предназначено для администраторов системы, а также для системных администраторов компьютерных сетей и сотрудников служб (подразделений) по поддержке программного и аппаратного обеспечения. В него включены следующие описания:

- инсталляция программного обеспечения;
- требования к сети Ethernet;
- особенности работы с программным обеспечением;
- порядок подготовки системы к работе;
- задание первоначальных установок функционирования системы;
- задание прав доступа пользователей к программному обеспечению системы;
- настройка сервера системы;
- работа с сервером системы.

СОСТАВ СИСТЕМЫ PERCO-S-20 «ШКОЛА»

Структурный состав системы PERCo-S-20 «Школа» показан на Рис. 1. Все технические средства и ПО системы PERCo-S-20 «Школа» работают в единой информационной среде передачи данных, реализованной на основе сети Ethernet.

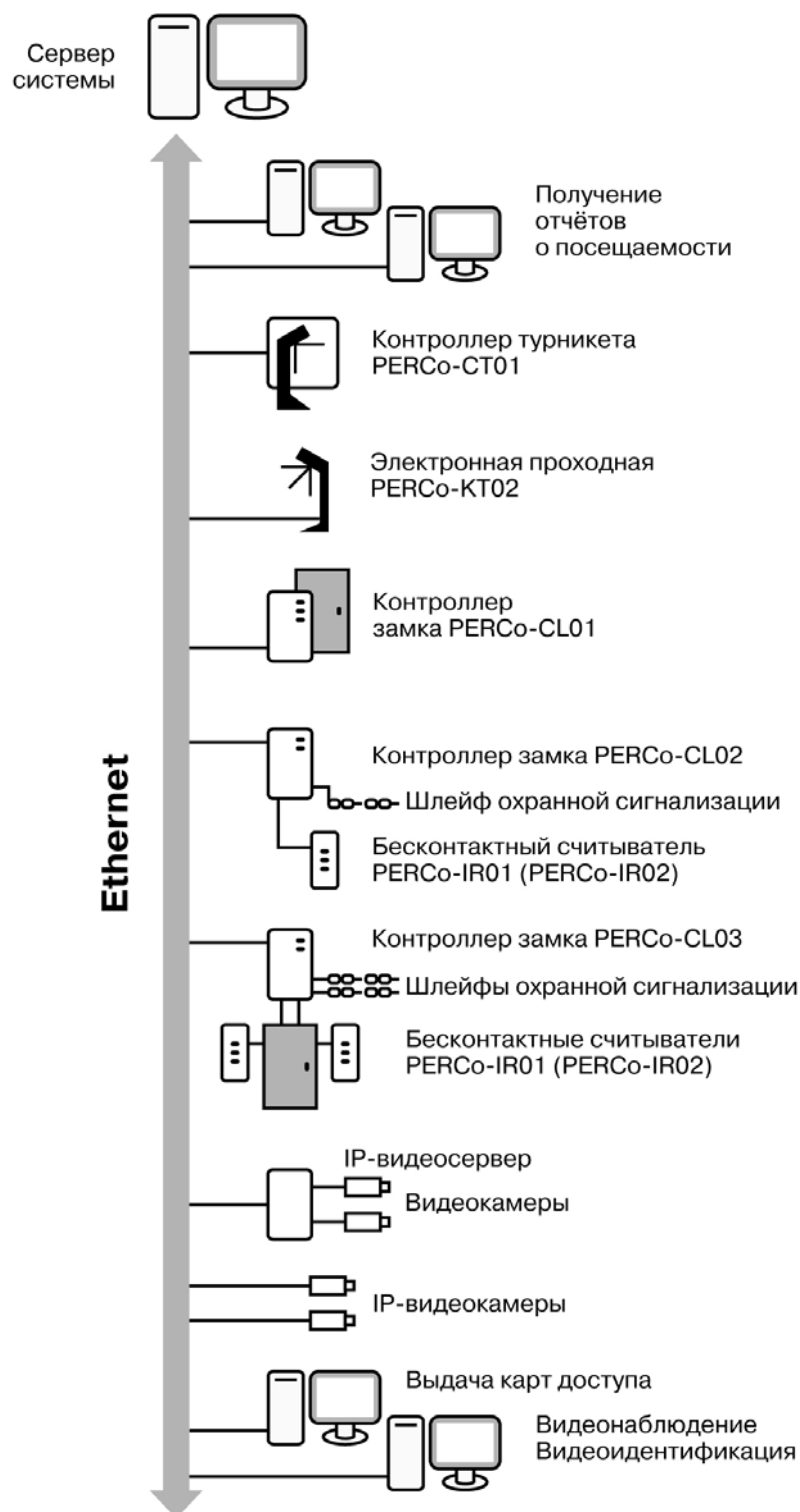


Рис. 1. Структурная схема системы PERCo-S-20 «Школа»

ПОРЯДОК ПОДГОТОВКИ СИСТЕМЫ К РАБОТЕ

Алгоритм подготовки системы к работе следующий:

- Разработать структурную схему системы.
- Выбрать компьютеры, где будет установлен сервер системы, сервер БД и будут работать модули ПО PERCo-S-20 «Школа».
- Провести инсталляцию ПО в соответствии с разработанной схемой.
- Запустить модуль «Центр управления PERCo-S-20 Школа» (**Пуск → Программы → PERCo → PERCo-S-20 School → Центр управления PERCo-S-20 Школа**). На данном этапе осуществить подключение к серверу БД и создать базу данных.
- Запустить модуль «Консоль управления PERCo-S-20 Школа» (**Пуск → Программы → PERCo → PERCo-S-20 School → Консоль управления PERCo-S-20 Школа**).
- Задать права доступа пользователей к разделам программного обеспечения системы и присвоить им индивидуальные пароли.
- Настроить контроллеры в соответствии с топологией Вашей сети Ethernet. При необходимости настроить DHCP сервер.
- Провести автоконфигурацию системы, т.е. операцию по автоматическому определению состава подключенной аппаратуры с дальнейшим заданием параметров работы подключенных устройств и привязкой этих устройств к объектам доступа. Если автоконфигурация осуществляется не администратором системы, то данный пункт выполняется только после задания прав доступа пользователей к программному обеспечению.

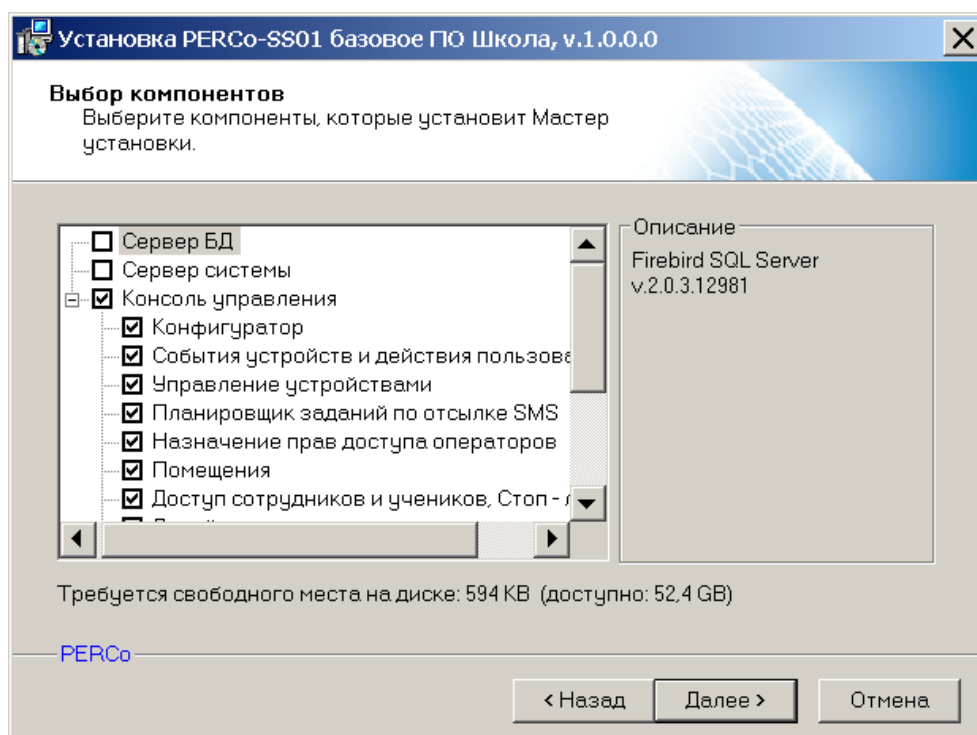
После проведения всех необходимых операций по настройке системы администратору рекомендуется задать свой собственный пароль для входа в нее. Данная процедура необходима для установки эксклюзивного права администратора изменять настройки системы.

ИНСТАЛЛЯЦИЯ ПО

Перед началом инсталляции программного обеспечения ознакомьтесь с разработанной структурной схемой системы безопасности. Определите, какие модули программного обеспечения на какие компьютеры будут установлены.

ИНСТАЛЛЯЦИЯ PERCO-SS01 БАЗОВОЕ ПО «ШКОЛА»

Вставьте компакт диск с дистрибутивом в привод CD-ROM. Должен автоматически запуститься инсталляционный модуль SetupSchoolBase.exe. Если этого не происходит — запустите данный модуль вручную. Следуйте указаниям мастера установки. Внимательно ознакомьтесь с предлагаемой информацией и лицензионным соглашением. После принятия лицензионного соглашения будет предложено выбрать устанавливаемые компоненты программного обеспечения:

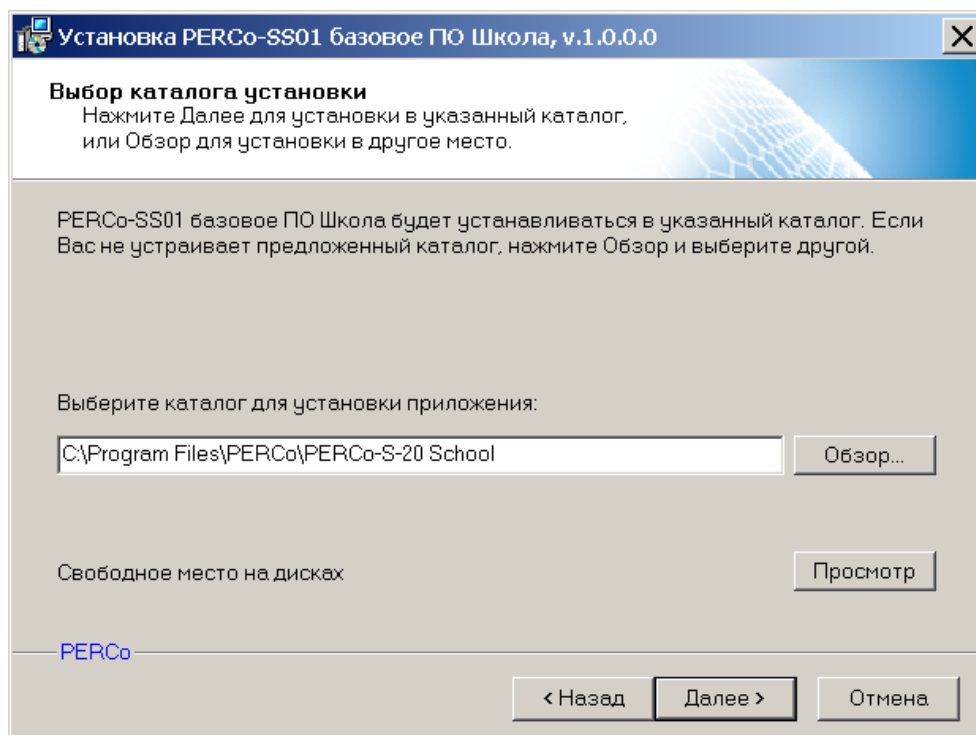


В соответствии с разработанной схемой системы безопасности выберите именно те компоненты программного обеспечения, которые должны быть установлены на данном компьютере. Щелкните на кнопке **Далее**.



ПРИМЕЧАНИЕ

Сервер системы как и сервер БД могут быть установлены только в единственном экземпляре в составе системы безопасности. Установка сервера системы автоматически приводит к установке сервера БД.



В открывшемся диалоговом окне укажите каталог, в который будет произведена установка программного обеспечения, и щелкните на кнопке **Далее**.

Следуйте указаниям мастера установки. После завершения установки программное обеспечение готово к работе.

Создайте или обновите Базу Данных. Инструкция по управлению Базами Данных приведена в п. [Управление серверами](#) данного Руководства Администратора.

УДАЛЕНИЕ PERCO-SS01 БАЗОВОЕ ПО «ШКОЛА»

Вставьте компакт диск с дистрибутивом в привод CD-ROM. Должен автоматически запуститься инсталляционный модуль SetupSchoolBase.exe. Если этого не происходит — запустите данный модуль вручную. Следуйте указаниям мастера установки.

Возможен другой способ удаления ПО: запустите Панель управления Windows (**Пуск** → **Программы** → **PERCo** → **PERCo-S-20** → **PERCo-S-20 School** → **Удалить PERCo-SS01 Базовое ПО Школа**). (Приведенный путь предопределен при инсталляции. Если в момент инсталляции был выбран другой каталог, приложение **Удалить PERCo-SS01 Базовое ПО Школа** будет открываться, соответственно, из выбранного при инсталляции каталога.) Далее следуйте указаниям мастера установки, который автоматически выбирает программу удаления.

ЛИЦЕНЗИИ

Все программное обеспечение, входящее в состав системы безопасности, требует после проведения инсталляции дополнительного ввода ключей активации.

В качестве аппаратного средства защиты программного обеспечения от несанкционированного использования применяются контроллеры, входящие в состав приобретенной системы безопасности. Выполнение функции аппаратного контроля

лицензий на программное обеспечение не влияет на остальные функциональные возможности контроллера.

Для упрощения процедуры регистрации программного обеспечения, а так же для ознакомления с возможностями программного обеспечения, в течение 30 дней с момента первой активизации сетевых модулей системы, программное обеспечение работает в ознакомительном режиме.

Под ознакомительным режимом понимается режим работы ПО с сохранением всех функциональных возможностей, но с выводом предупреждающего напоминания и указанием времени оставшегося до окончания ознакомительного периода. По прошествии 30 дней доступ к неактивированным сетевым модулям будет запрещен.

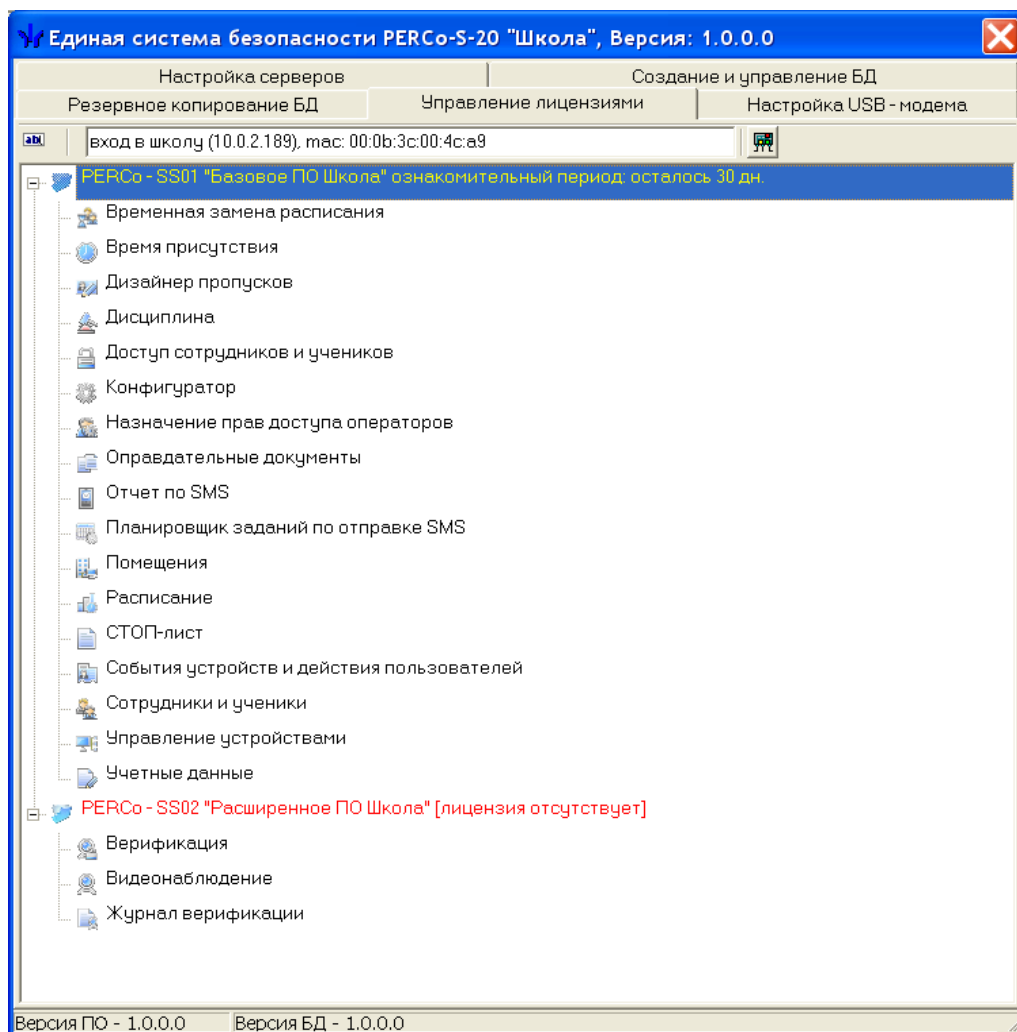
Для получения ключей активации приобретенного программного обеспечения выберите один из контроллеров, входящих в систему безопасности, который будет выполнять функцию аппаратного контроля лицензий на программное обеспечение; заполните соответствующим образом заявку на приобретение лицензии, и отправьте его в компанию PERCo.

После получения лицензионного соглашения, содержащего ключи активации программного обеспечения, введите их в программное обеспечение. Ввод ключей активации производится на вкладке **Управление лицензиями** в модуле Центр управления PERCo-S-20 Школа. Более подробная информация о работе с этим модулем приведена в п. [Управление серверами](#) данного руководства.

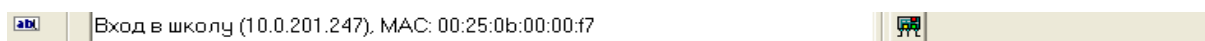
Для запуска Центра управления PERCo-S-20 «Школа» запустите (**Пуск → Программы → PERCo → PERCo-S-20 School → Центр управления PERCo-S-20 Школа**). Убедитесь, что в данный момент сервер БД и сервер системы запущены и работают. Перейдите на вкладку **Управление лицензиями**:

Для ввода лицензии укажите контроллер, MAC-адрес которого был внесен Вами в лицензионное соглашение. Для этого воспользуйтесь кнопкой, расположенной в верхней части программного окна .

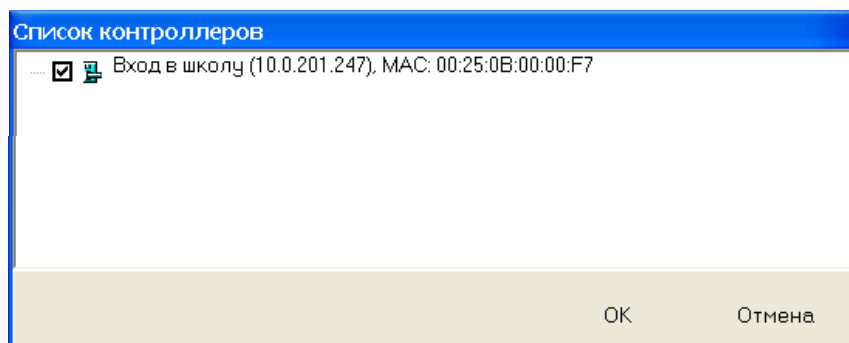
После щелчка на ней откроется диалоговое окно выбора:



В этом окне отметьте выбранный Вами раньше контроллер и щелкните на кнопке «**ОК**», что приведет к закрытию диалогового окна и отображению имени выбранного контроллера в поле в верхней части рабочего окна:



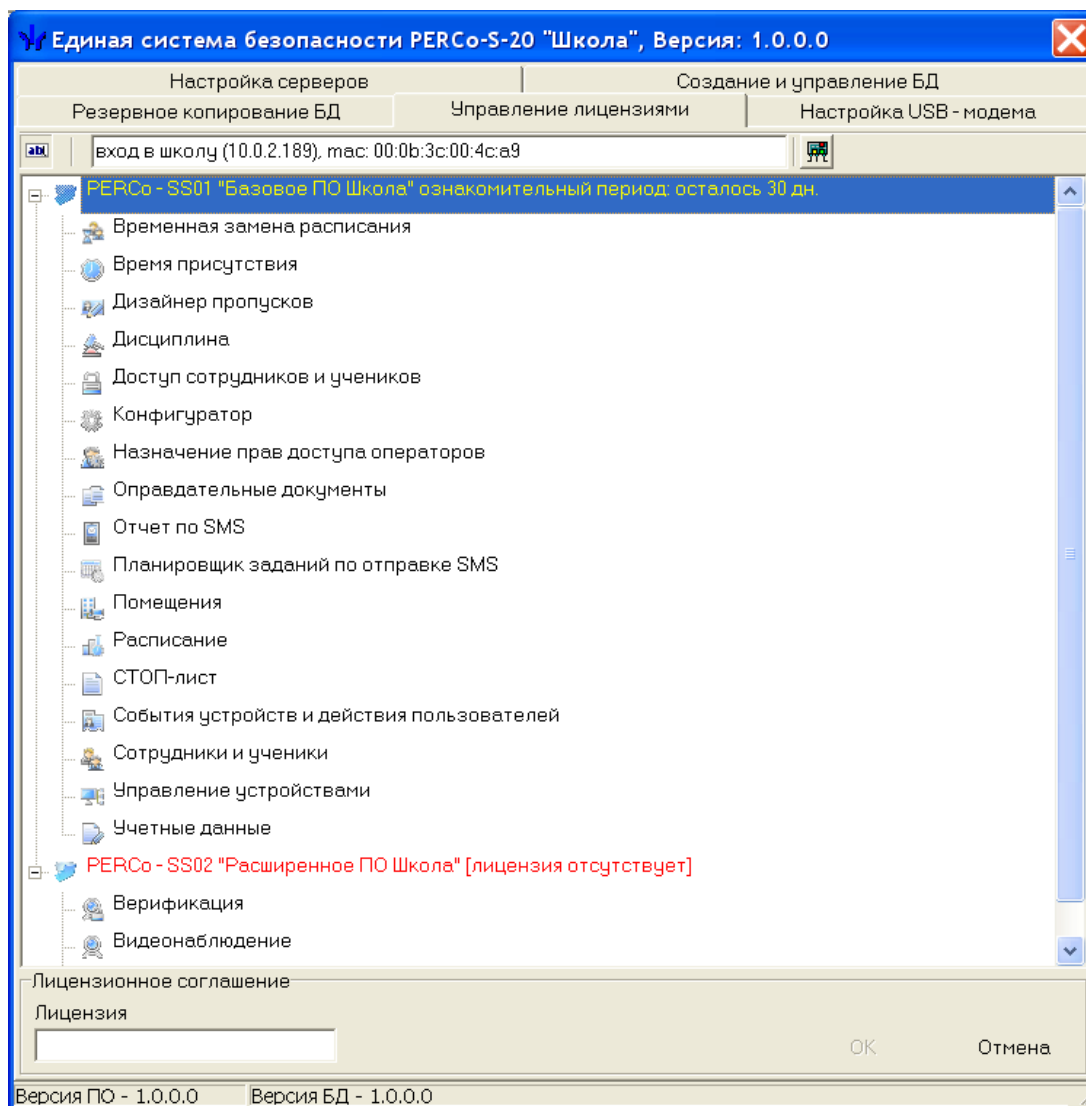
После выбора контроллера выделите в списке тот программный модуль, лицензию на который Вы собираетесь ввести, и щелкните на кнопке **Изменить лицензию**. При этом становится доступным строка ввода ключа активации:





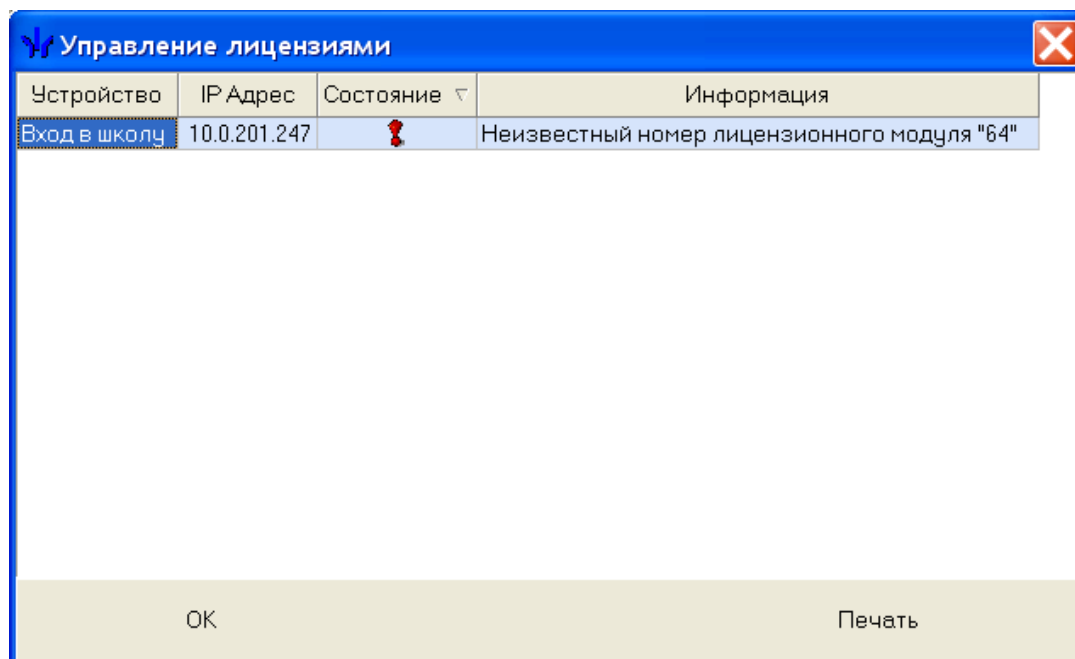
ПРИМЕЧАНИЕ

Код активации вводится без разделителей. Выбранный Вами контроллер должен находиться во включенном состоянии, и быть подключенным к программному обеспечению. Для проверки наличия связи между программным обеспечением и выбранным контроллером можно воспользоваться разделом «Управление устройствами».

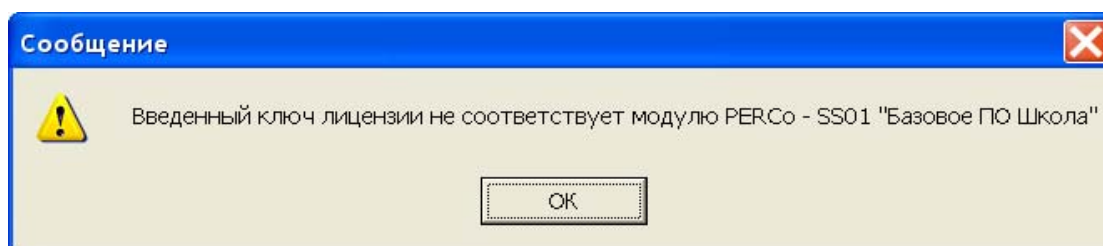


Введите код активации и щелкните на кнопке . После этого программное обеспечение автоматически осуществит передачу введенного кода активации на проверку в выбранный контроллер. При положительном ответе от контроллера рядом с названием выбранного модуля отображается информации о количестве активированных копий.

В случае невозможности связаться с выбранным контроллером программное обеспечение выдаст сообщение о невозможности подключения и проверки правильности введенного ключа активации:



В случае если Вы ошиблись при вводе ключа активации, и система не может правильно декодировать его (то есть он не соответствует выбранному модулю и/или контроллеру), программное обеспечение выдаст сообщение об ошибке регистрации ключа активации:



В случае выдачи ошибки проверьте, что контроллер в данный момент находится на связи с программным обеспечением, что Вы не ошиблись при вводе ключа активации. И повторите попытку.



ПРИМЕЧАНИЕ

Выбранный Вами контроллер всегда будет использоваться для проверки введенных ключей активации! Смена контроллера приведет к тому, что все введенные ранее лицензии будут недействительны!

ОБЩИЕ СВЕДЕНИЯ

Для функционирования сетевых контроллеров необходима сеть Ethernet 10-BaseT, 100-BaseTX или 1000-BaseTX. Для передачи данных используются непосредственно IP-адреса контроллеров, а также UDP протокол. Наличие таких серверов или служб, как DNS и WINS, не требуется.

С точки зрения правильной настройки системы передачи данных в существующей топологии сети школы, эксплуатирующей систему PERCo-S-20 «Школа», необходимо

понимание реализованного механизма передачи данных. Ниже представлена информация, которая потребуется сетевым администраторам при наличии в организации нескольких подсетей, межсетевых маршрутизаторов и экранов и т.п.

Для обмена данными в системе используется следующий стек протоколов (Рис. 2):

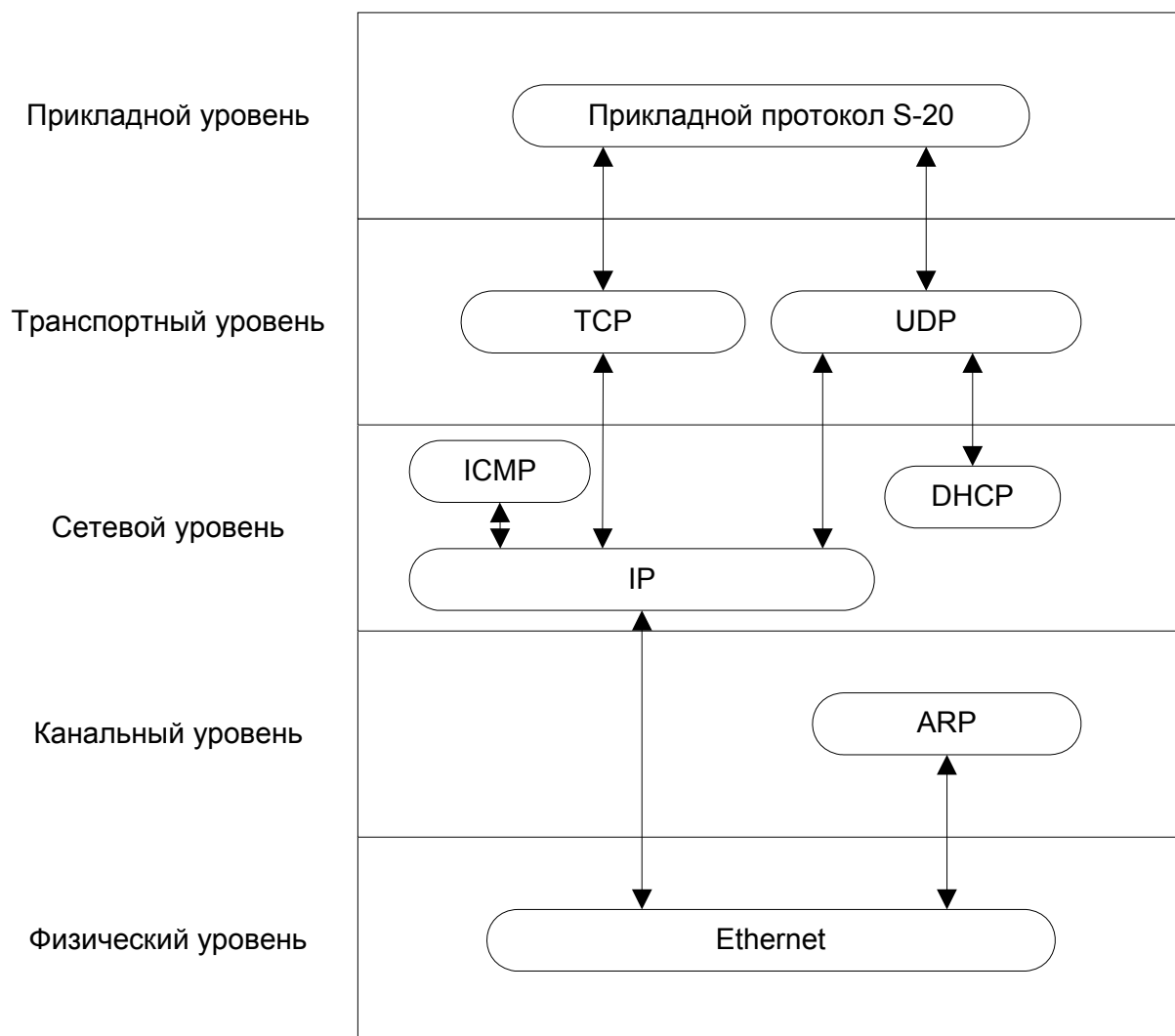


Рис. 2. Стек протоколов, используемых для обмена в системе

Также для передачи данных используются следующие порты:

Табл. 1

Протокол	Порт	Назначение
UDP	18900	конфигурация сетевых параметров контроллера
	18901	широковещательные кадры (только между контроллерами) внутри подсети
TCP	18902	порт контроллера для конфигурации, управления и диагностики
	18903	порт контроллера для приема журнала регистрации
	18904	порт контроллера для регистрации индицирующего устройства
	18905	порт контроллера для регистрации верифицирующего устройства
	18906	порт контроллера для приема и анализа мониторинга

Перечисленные в Табл. 1 порты должны быть свободны, и не использоваться другими приложениями и службами в сети школы. Также, если Вы используете персональные Firewall-ы или встроенные в Windows XP, то в их конфигурации должны учесть эти данные.

С точки зрения конфигурирования сетевых коммутаторов и подобного оборудования, следует иметь в виду, что контроллерами и сервером системы PERCo-S-20 помимо адресной передачи пакетов используется и широковещательная передача. Однако, «достаточным» условием будет возможность прохождения широковещательных пакетов в пределах своей подсети, трансляции в другие подсети не требуется. При установке контроллеров в другие подсети для обеспечения связи с ПО PERCo-S-20 «Школа» их адреса в других подсетях придется заносить в ПО PERCo-S-20 «Школа» вручную.

Сетевые контроллеры не поддерживают фрагментацию IP-пакетов. Поэтому, если у Вас в школе довольно разветвленная сеть, использующая роутеры, концентраторы и сетевые модемы, то удостоверьтесь, что IP-пакеты на всем протяжении от сервера системы PERCo-S-20 до контроллера не фрагментируются:

1. Убедитесь на примере компьютера с сетевыми настройками аналогичными настройкам контроллера, который предполагается установить, что между точками подключения сервера системы PERCo-S-20 и контроллера существует связь (маршрутизация настроена правильно, нет обрывов кабеля и т.п.).

Для проверки связи (на примере ОС Windows):

а) щелкните на панели инструментов **Пуск** → **Выполнить** → в открывшемся окошке введите *cmd.exe*;

б) в появившейся консоли введите

ping XX.XX.XX.XX,

где (XX.XX.XX.XX – адрес вашего компьютера, т.е. тот адрес, который планируется установить контроллеру).

Если связь есть, то вы увидите строки вида:

Ответ от 193.124.71.56: число байт=32 время<10мс TTL=128.

Если связи (ответа) нет, то проверьте правильность настройки маршрутизации в Вашей сети.

2. Подключите настроенный (см. ниже) контроллер.

3. «Пропингуйте» контроллер с порта, к которому планируется подключать сервер системы PERCo-S-20.

Для этого в этой же консоли введите:

ping XX.XX.XX.XX -l 576.

Если связь есть и стандартные минимальные пакеты (576 байт) не фрагментируются, то вы увидите строки вида:

Ответ от 193.124.71.56: число байт=576 время<10мс TTL=128.

В данном случае можно утверждать, что IP-пакеты размером меньшим 576 байт не фрагментируются, и выбранное Вами подключение должно работать.

Если положительный ответ получить не удастся, то вероятнее всего на пути следования IP-пакетов находится сетевое коммутирующее оборудование, фрагментирующее IP-пакеты, которые размером меньше 576 байт. Проверьте настройки этого оборудования, при возможности увеличьте размер MTU. Обычно этот параметр обозначается как *MaxMTU* или *IPMTU*.

Если у Вас возможны несколько вариантов коммутации, то воспользуйтесь командой:

ping XX.XX.XX.XX -l 576 -t.

Коммутируя разными способами, смотрите на время ответа, выбирая соединение, дающее максимально быстрый ответ.

НАСТРОЙКА КОНТРОЛЛЕРА

Помимо определения местоположения контроллера как физически, так и в сети, настройте сам контроллер.

Для этого:

- Задайте IP-адрес и выберите режим получения адреса, согласовав его с работой Вашей сети.
- Сконфигурируйте контроллер с помощью раздела Конфигуратор (см. Руководство пользователя по разделу Конфигуратор), определив его целевые параметры.

Каждый контроллер имеет следующие предопределенные (заводские) сетевые настройки:

IP-адрес : 10.x.x.x

Шлюз : 10.0.0.1

Маска сети : 255.0.0.0

MAC-адрес : xx xx xx xx xx xx (уникальный, неизменяемый при настройках).

Конкретные для каждого контроллера значения (вместо символа «х») указываются в паспорте на изделие и на наклейке на корпусе контроллера.

После задания настроек (*IP-адрес, шлюз, маска сети*) при конфигурировании контроллера в силу вступают заданные *пользовательские настройки*.

Настройка контроллера производится в зависимости от наличия в сети организации DHCP сервера. Главное, что нужно учитывать при задании сетевых настроек и последующей конфигурации самой системы PERCo-S-20 «Школа» - это необходимость обеспечения:

- уникальности сетевых адресов контроллеров в своей сети;
- предотвращения смены контроллерами своих адресов (после конфигурации системы PERCo-S-20 «Школа») вследствие работы сервера DHCP.

РЕЖИМ ПОЛУЧЕНИЯ АДРЕСА

Режим работы по получению контроллером адреса задается с помощью устанавливаемых на плате перемычек на – **XPI**. Расположение перемычек для контроллеров показано на Рис. 3.

Результаты изменений положения перемычек вступают в силу только при перезапуске контроллера путем отключения и повторного включения питания на нем..

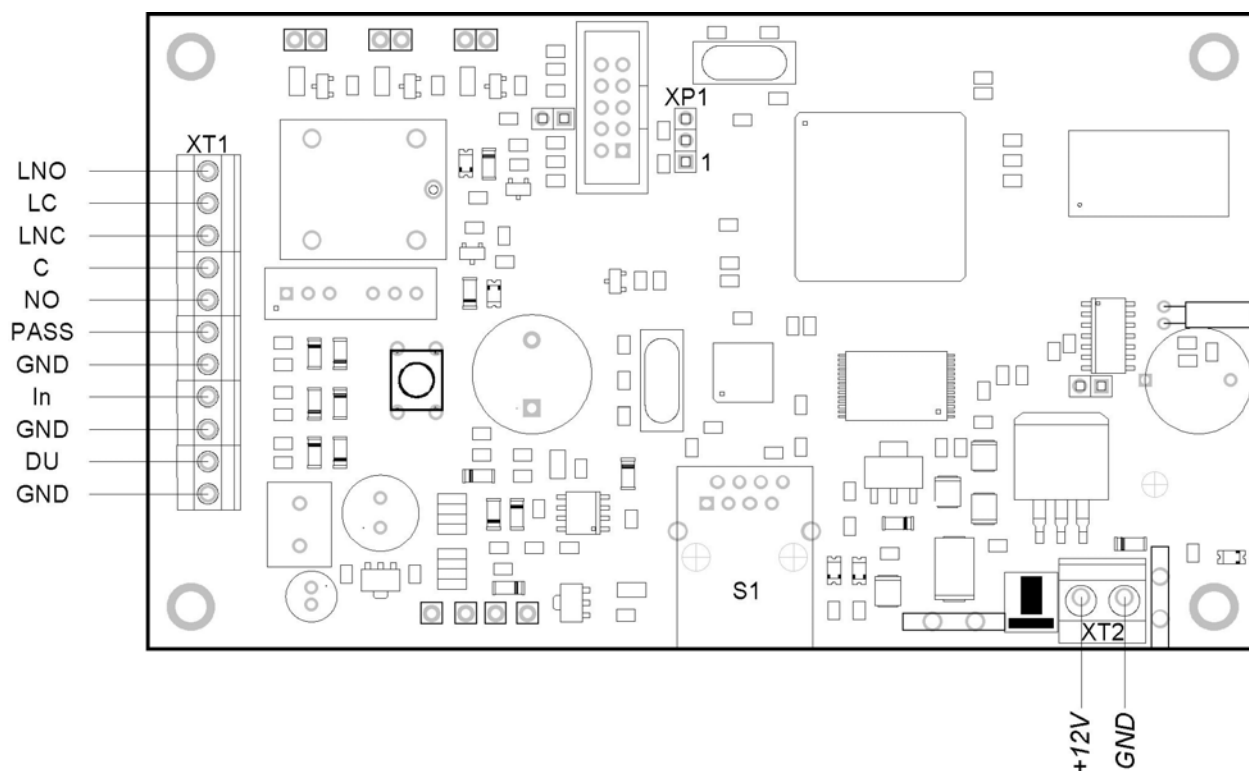
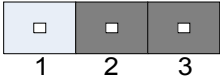
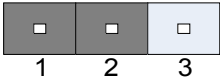
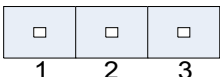


Рис. 3. Монтажные схемы контроллеров системы PERCo-S-20

Варианты перемычек на контроллерах

№	Расположение перемычек на XP1	Режим
1.		Установка заводских параметров
2.		Работа с DHCP, с предложением DHCP серверу присвоить предлагаемый (пользовательский) адрес. При первом запуске заводской (если пользовательский не был введен ранее), потом – ранее выделенный сервером DHCP
3.		Установка пользовательских параметров. Если их нет, то установка заводских параметров

Настройка без DHCP

Настройка производится с помощью персонального компьютера с установленным ПО PERCo-S-20 «Школа». Обеспечьте связь по сети Ethernet контроллера и компьютера с установленным сервером системы PERCo-S-20. Для обеспечения данной связи контроллер с установленными сетевыми настройками подключается в тот же сегмент сети или непосредственно к сетевому разъему сетевой карты компьютера.

Для обеспечения этого условия:

- Добавьте (см. Рис. 4) новый IP-адрес на сетевой интерфейс Вашего персонального компьютера с установленным ПО PERCo-S-20 «Школа». Или измените существующие IP-адрес (например, 10.0.0.1) и маску сети на те, которые указаны в паспорте на контроллер. Сделайте это соответствующим для операционной системы образом.

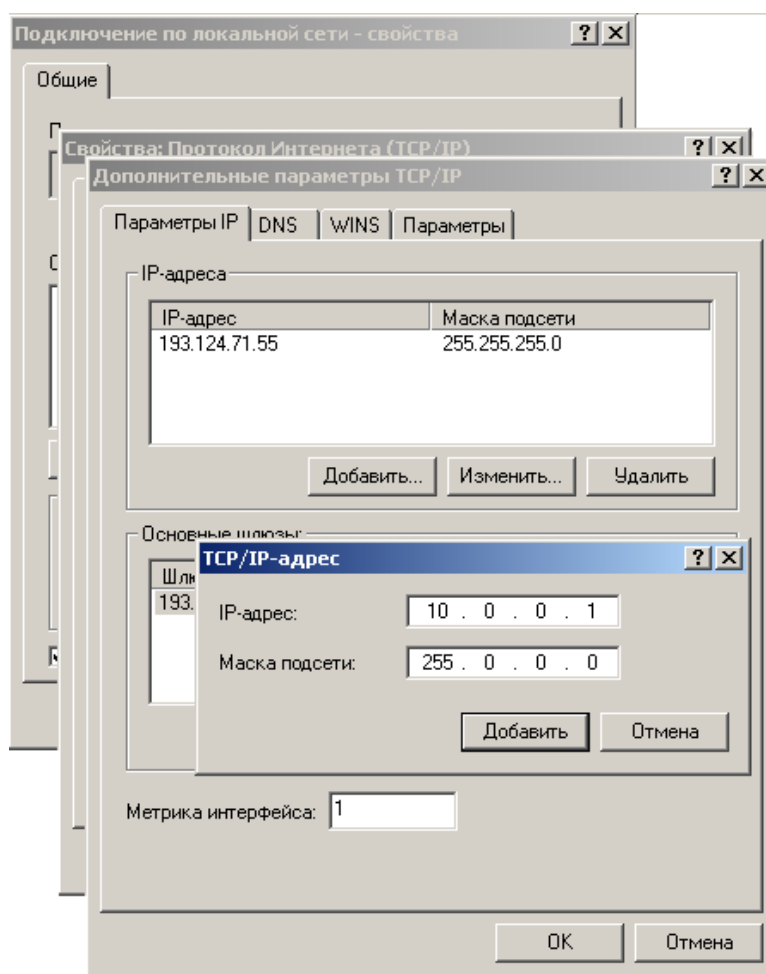


Рис. 4. Добавление нового IP-адреса

- Установите переключки по 4-му варианту (см. Табл. 2).
- Подключите контроллер к сети (в тот же сегмент) или непосредственно к сетевому разъему сетевой карты компьютера.

Если при подключении контроллера непосредственно к разъему RJ-45 (порт MDI-X) связь с контроллером не удалось установить, то

используйте сетевой кабель с перекрестным соединением пар. Такой кабель, например, применяют при соединении концентраторов через стандартный порт MDI-X.

- Включите контроллер. Произведите настройку согласно п. «[Конфигурация контроллеров](#)».

У контроллера достаточно сконфигурировать только сетевые настройки.

- Установите контроллер на выбранное место работы.

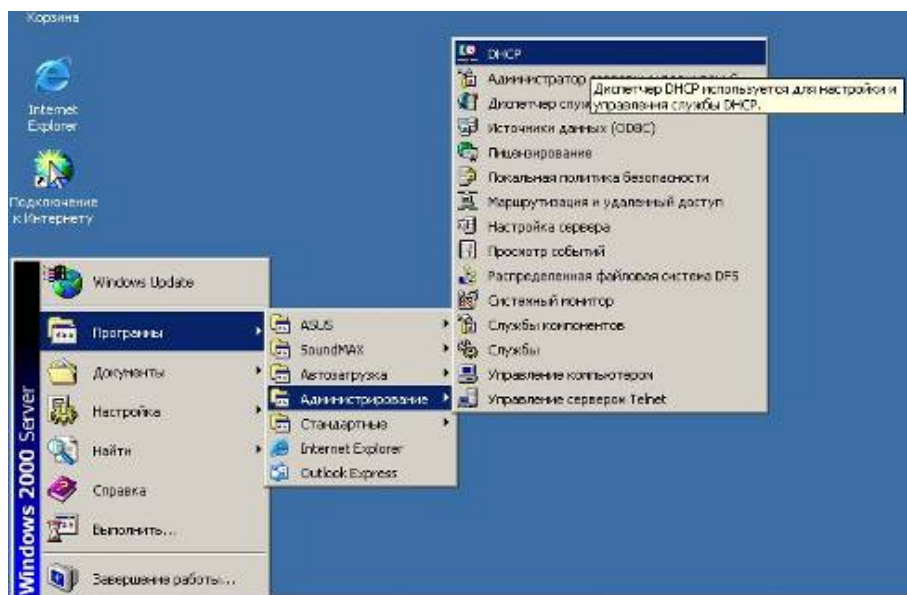
Настройка с DHCP

Настройка DHCP сервера, установленного в сети школы, сводится к резервированию диапазона адресов, выделяемых под контроллеры, и к привязке MAC-адреса контроллера и назначению контроллеру IP-адреса. Следует обратить внимание, что при настройке (перемычками на плате) контроллера на режим работы с DHCP изменения настроек, сделанные через Конфигуратор, не будут иметь силы.

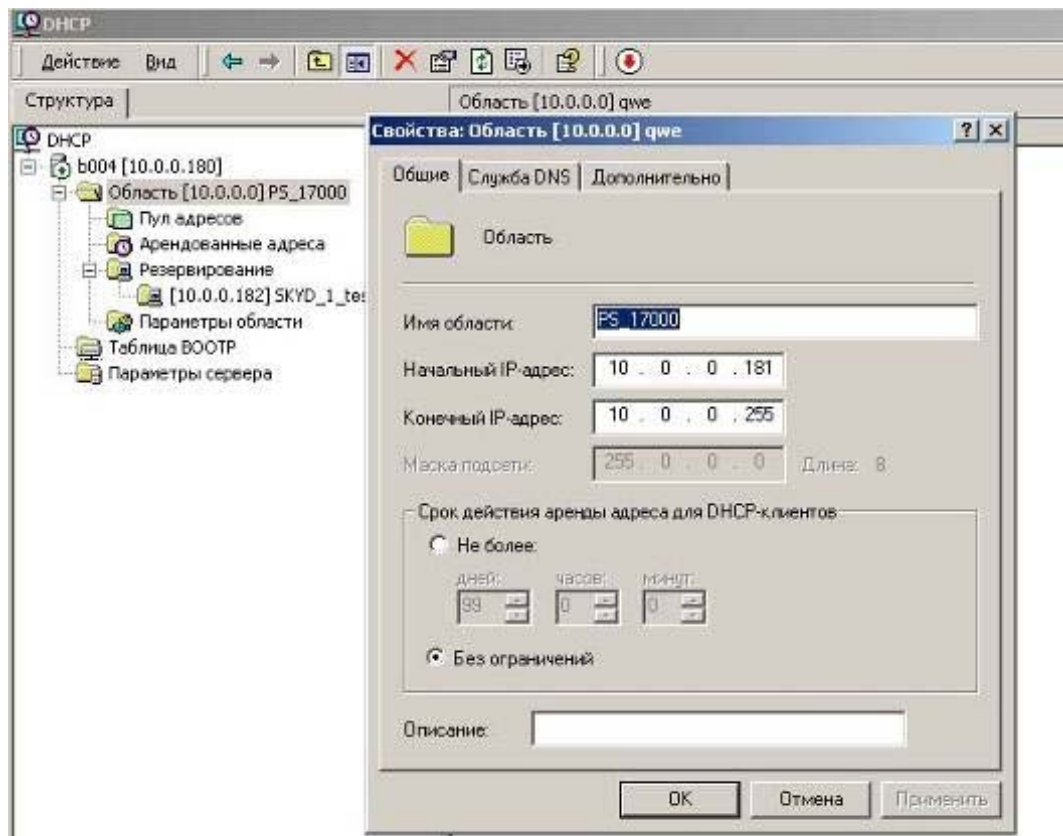
ОС Windows

Описание настройки приведено на примере Windows 2000. Для других операционных систем смысл остается таким же.

- Запустите DHCP сервер:



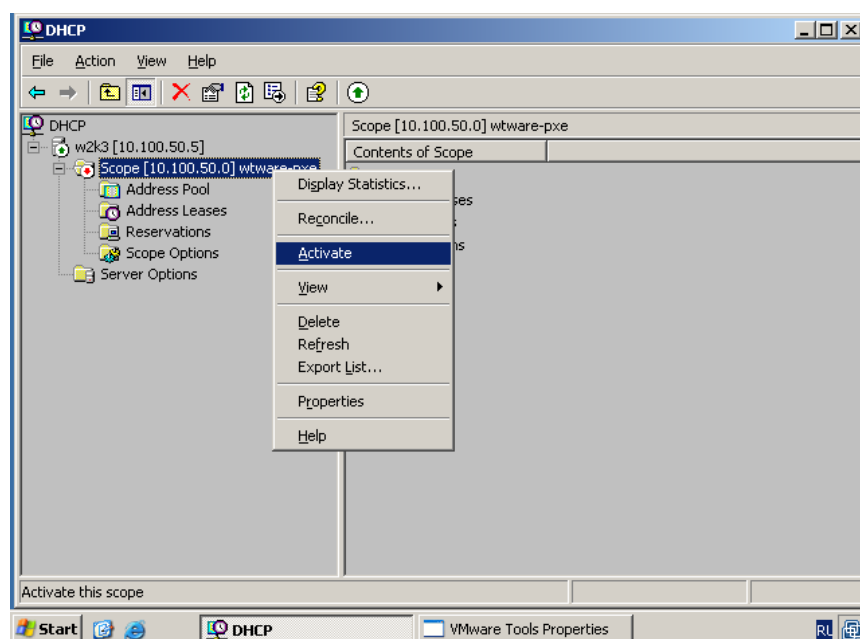
- Создайте область адресов для контроллеров системы PERCo-S-20:



Название области и описание могут быть любыми. Это информация не для системы, а для системного администратора. Лучше, если название достаточно информативно, чтоб не вспоминать потом, что настраивается в этой области.

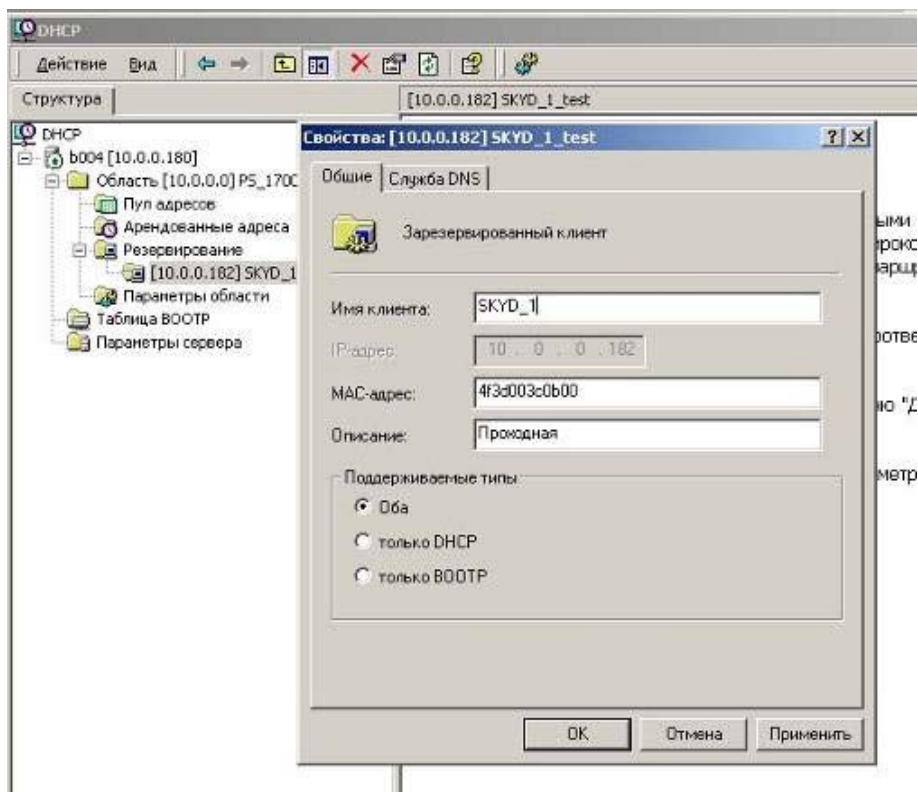
Рекомендуется делать область несколько больше, чем число контроллеров, которое планируется использовать. Также задавайте такую область адресов, которая не будет включать в себя уже существующие машины с фиксированными адресами.

- Последний и *обязательный* шаг - активация области:



После этого Ваш DHCP сервер сможет предоставить информацию, необходимую контроллеру для получения IP-адреса.

- Проведите резервирование адресов своих контроллеров. Для этого задайте IP-адрес из выбранной Вами области и поставьте его в соответствии с MAC-адресом контроллера, указанном в паспорте.
- Для удобства добавьте описание.



Данную операцию повторите для всех контроллеров, которые планируется установить в Вашей сети.

- Установите перемычки по 2-му варианту (см. Табл. 2).
- Подключите контроллеры к сети и включите их.

Если вы не ошиблись при вводе, то все контроллеры будут отображаться в списке арендованных адресов.

- Обязательно проверьте, чтобы в столбце о времени аренды адреса находилась информация об активном резервировании.

ОС Linux

Если у Вас сервер DHCP установлен на ОС Linux, то настройка сведется к редакции файла конфигурации «демона» сервера DHCP (dhcpd). Конфигурационным файлом для dhcpd является `/etc/dhcp.conf`. Не забудьте, что, чтобы внесенные Вами в файл `/etc/dhcp.conf` изменения вступили в силу, «демон» (dhcpd) необходимо остановить и запустить снова.

При этом можно использовать команду `/etc/rc.d/init.d/dhcpd stop` для остановки «демона», и команду `/etc/rc.d/init.d/dhcpd start` для его запуска.

Примерный вариант файла конфигурации показан ниже:

```
# Подсеть 10.100.0.0, маска сети 255.255.255.0

subnet 10.100.0.0 netmask 255.255.255.0 {

# маска подсети 255.255.255.0

option subnet-mask 255.255.255.0;

...

# диапазон адресов для контроллеров

# 10.100.0.10-10.100.0.254

range 10.100.0.10- 10.100.0.254;

...

# описание контроллеров (proxod_1, ..., office_room_101)

# обратите внимание на то, что вы должны использовать

# IP-адрес из указанного Вами диапазона

host proxod_1 {

hardware ethernet XX:XX:XX:XX:XX:XX;

fixed-address 10.100.0.50;

}

...

host office_room_101 {

hardware ethernet XX:XX:XX:XX:XX:XX;

fixed-address 10.100.0.37;

}

...

}
```

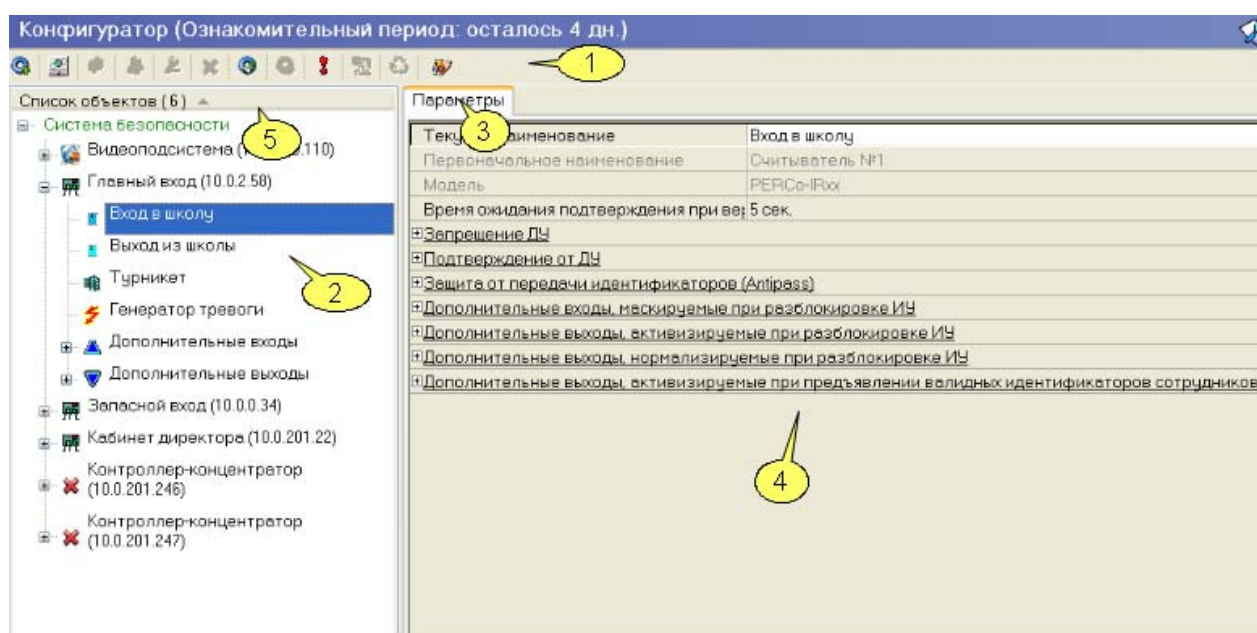
Опции настроек маршрутизатора, домена, широковещательного адреса, DNS и т.д. прописываются при необходимости (для более полной информации о вариантах конфигурации воспользуйтесь командой *man dhcpd.conf*).

ОСОБЕННОСТИ РАБОТЫ СТЕКА ПРОТОКОЛА TCP/IP В WINDOWS XP SP1, SP2, SP3

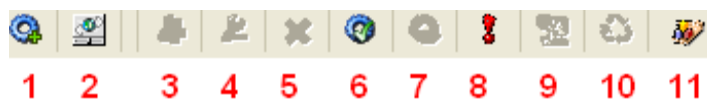
В операционной системе Windows XP существует ограничение на количество попыток одновременных TCP-подключений. Количество таких попыток по умолчанию равно 10 и введено для защиты от вирусов и DoS-атак. Если Сервер системы установлен на компьютер с Windows XP, то следует пропатчить драйвер TCPIP.SYS на количество таких попыток равное 100. Один из возможных патчей находится по адресу http://half-open.com/download_ru.htm. О наличии ограничения на количество попыток одновременных TCP-подключений можно судить по записям в журнале событий системы. Запустите Event Viewer (например через Control Panel — Administrative Tools; или Пуск — Выполнить — EventVwr.msc). Каждое сообщение вида «EventID 4226: Достигнут предел безопасности для TCP/IP, налагаемый на количество попыток одновременных TCP-подключений.» говорит о том, что такое ограничение сработало.

КОНФИГУРАЦИЯ КОНТРОЛЛЕРОВ

Раздел Конфигуратор предназначен для описания параметров функционирования устройств и программного обеспечения системы безопасности PERCo-S-20. Для активизации раздела щелкните на кнопке раздела Конфигуратор. Рабочее окно раздела откроется в основной части окна Консоли управления.

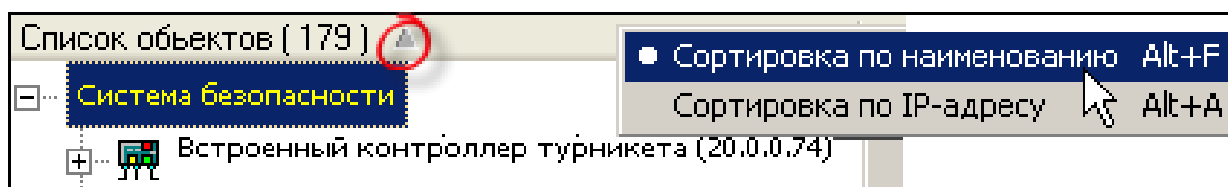


1. Функциональные элементы раздела .



- 1 — Провести конфигурацию
- 2 — Добавить новое устройство
- 3 — Добавить группу ресурсов
- 4 — Удалить устройство
- 5 — Исключить из конфигурации/включить в конфигурацию
- 6 — Передать параметры
- 7 — Передать измененные параметры системы
- 8 — Отображать скрытые устройства
- 9 — Изменение пароля
- 10 — Изменение сетевых настроек
- 11 — Получить информацию о версиях прошивок

- 2. Рабочая область раздела Конфигуратор. Содержит в себе список доступных для использования устройств.
- 3. Вкладка раздела Конфигуратор.
- 4. Панель параметров вкладки.
- 5. Кнопка сортировки списка.



Щелкните правой кнопкой мыши на кнопку сортировки списка и выберите критерий сортировки: по наименованию или по IP-адресу объекта. В зависимости от выбора щелчком мыши на кнопку сортировки устройства сортируются в прямом () и обратном алфавитном порядке () или по нарастанию () и убыванию IP-адреса ().

Проведение конфигурации

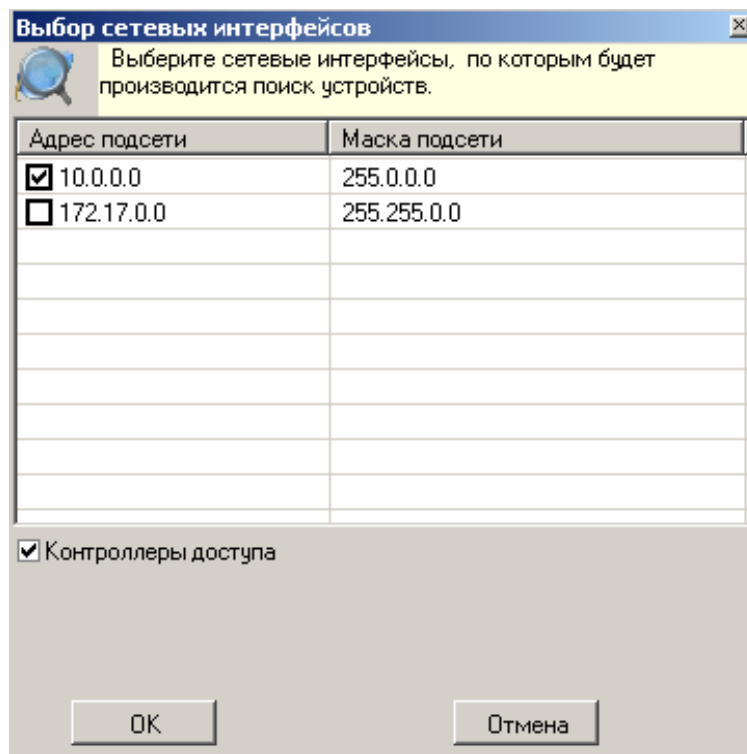
Для нормального функционирования системы безопасности необходимо определить ее состав и произвести соответствующие настройки аппаратуры.

Самым простым вариантом работы по данному сценарию является использование заданных при производстве контроллеров IP-адресов и задание IP-адресов из той же подсети в стеке IP-адресов персональных компьютеров, на которых установлено программное обеспечение системы.

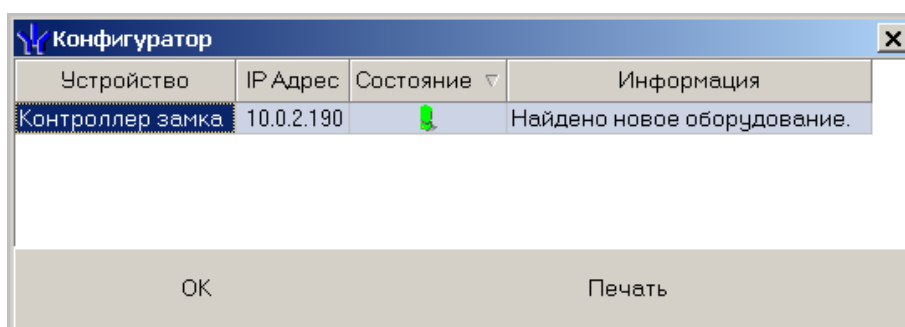
Если все вышесказанное выполнено, произведен монтаж контроллеров системы, при помощи команды “ping” проверено прохождение IP-пакетов с компьютера с установленным сервером системы, можно приступить к проведению конфигурации системы безопасности.

Аппаратно-программный состав системы может быть определен автоматически или добавлен вручную.

Для проведения автоматической конфигурации щелкните на кнопке **Провести конфигурацию** . На экран будет выведено окно выбора сетевых интерфейсов:

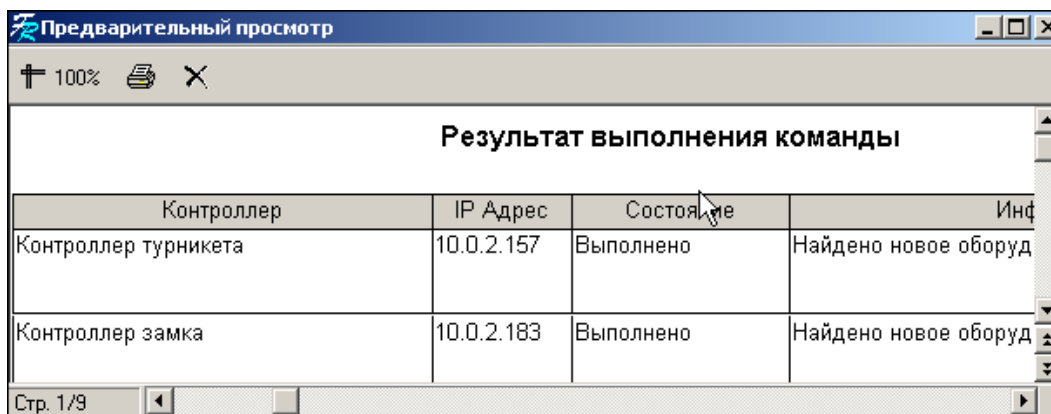


Выберите адрес и маску подсети, где будет производиться поиск устройств, подтвердив свой выбор щелчком на кнопке «**OK**». Через некоторое время откроется окно с результатом запроса, сообщающее, есть ли новое оборудование в конфигурации:



После закрытия окна щелчком на кнопке «**OK**» или кнопке найденное оборудование будет отображено в списке рабочей области раздела Конфигуратор.

Кнопка **Печать** выведет на экран окно предварительного просмотра результатов выполнения команды:



Масштаб —  100% — предназначен для настройки изображения документа на экране.

Печать отчёта —  — для вывода документа на печать.

Выход — для выхода из режима предварительного просмотра в окно раздела Конфигуратор.

В случае если новое оборудование не будет обнаружено, в столбце Информация в окне с результатами запроса на проведение конфигурации будет сообщение о том, что новое оборудование не найдено.

Проанализируйте полученную информацию, а именно проверьте, все ли контроллеры были найдены в результате проведения конфигурации.

Если какой либо из контроллеров не был найден, проверьте правильность его монтажа, прохождение IP-пакетов к этому контроллеру от компьютера с установленным сервером системы и повторите конфигурацию.

Если контроллер так и остался не найденным, попробуйте добавить его в конфигурацию вручную.

Перед началом добавления убедитесь, что оборудование смонтировано в соответствии с инструкцией по монтажу и включено.

Добавление нового устройства

В случае если в результате проведения автоматической конфигурации оборудования, какое либо устройство не было определено, Вы можете добавить его в ручном режиме. Для добавления нового устройства:

1. Щелкните на кнопке **Добавить новое устройство** —  . Откроется диалоговое окно:

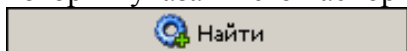
Поиск нового устройства

Категория: Контроллеры доступа, КБО, ППКОП

IP-адрес:

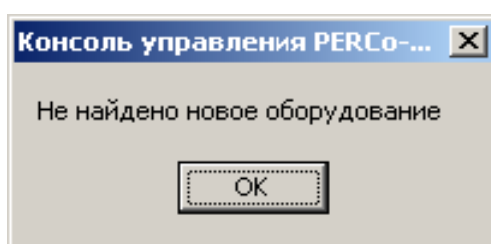
Найти

2. В списке Категория выберите Контроллер доступа .
3. В строку IP адрес введите IP-адрес устройства формате XXX.XXX.XXX.XXX, который указан в его паспорте и на наклейке. Станет активна кнопка



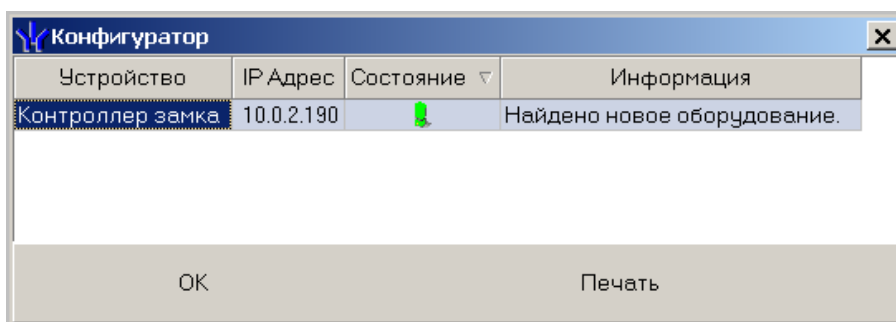
4. Щелкните на кнопке Найти. В рабочем окне в списке устройств отобразится новое устройство.

В случае если новое устройство не будет найдено, будет выведено диалоговое окно:



Это может быть связано с тем, что-либо контроллер выключен, либо не правильно настроены параметры локальной сети на компьютере.

Если оборудование обнаружено, то откроется окно сообщения:



Щелкните на кнопке «**ОК**». Найденное оборудование будет добавлено в конфигурацию системы.

После того, как все контроллеры будут добавлены, перейдите к описанию параметров их функционирования [Описание параметров функционирования контроллеров](#).

После описания параметров функционирования найденного оборудования передайте измененные параметры в аппаратуру с помощью кнопки **Передать измененные**

параметры —

Описание параметров функционирования контроллеров доступа (серия CL01, CL02, CL03, CT01, KT02)

Подробная информация о параметрах функционирования контроллеров системы безопасности приведена в техническом описании системы безопасности.

Ниже будут приведены общие рекомендации, проиллюстрированные примерами задания тех или иных параметров контроллеров доступа.

Дополнительный вход

Каждый контроллер доступа, в зависимости от своего типа, имеет от одного до четырех дополнительных входов.

Дополнительные входы контроллеров могут быть использованы для наблюдения за состоянием внешнего оборудования, подключенного к ним, и для подключения кнопок сброса тревоги.

В зависимости от того, какое внешнее оборудование подключено к дополнительному входу, существуют следующие варианты описания параметров его работы:

- При условии, что к данному дополнительному входу не подключено никакое внешнее оборудование, менять параметры работы дополнительного входа не нужно.
- **Нормальное состояние контакта** (нормально замкнут / нормально разомкнут). Этот параметр зависит от типа подключенного оборудования и указывает контроллеру на то, какое значение уровня сигнала на данном дополнительном входе он должен воспринимать как нормальное.
- Тип дополнительного входа – **Обычный**. Означает что к данному дополнительному входу подключено внешнее оборудование, состояние которого должно контролироваться контроллером. При выборе этого типа можно так же указать алгоритм действий контроллера при получении управляющего воздействия от подключенного оборудования, а именно:

Текущее наименование	Дополнительный вход №1
Адрес	1
Первоначальное наименование	Дополнительный вход №1
Нормальное состояние контакта	Разомкнут
Тип	Обычный
Обычный	
Дополнительные входы, маскируемые при активизации	
Критерий маскирования	На указанное время
На указанное время	
Время	3 сек.
Дополнительный вход №2	☒
Дополнительные выходы, активизируемые при активизации	
Критерий активизации	На время срабатывания
Дополнительный выход №1	☒
Дополнительный выход №2	☐
Дополнительные выходы, нормализируемые при активизации	
Критерий нормализации	На время срабатывания и после срабатывания
На время срабатывания и после срабатывания	
Время	250 мс.
Дополнительный выход №1	☒
Дополнительный выход №2	☐
Дополнительные выходы, реагирующие через группу ресурсов	
Дополнительный выход №4	☒
Дополнительный выход №5	☐

- **Дополнительные входы, маскируемые при активизации.** Этот параметр позволяет указать, какие именно дополнительные входы контроллера должны быть маскированы, т.е. не воспринимать управляющий сигнал от внешнего оборудования, при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте флажки тех дополнительных входов, которые должны быть маскированы. Кроме этого, укажите временной критерий маскирования, который может быть одним из трех видов:

Критерий маскирования	На указанное время
На указанное время	На указанное время
Время	На время срабатывания
Дополнительный вход №2	На время срабатывания и после срабатывания
	☒

- ✓ **На указанное время** – выбранные дополнительные входы будут маскированы на указанное время.
- ✓ **На время срабатывания** – выбранные дополнительные входы будут маскированы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.
- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные входы

- **Дополнительные выходы, активизируемые при активизации.** Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть активизированы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть активизированы. Кроме этого, укажите временной критерий активизации, который может быть одним из трех видов:

☐ Критерий активизации	На указанное время
☐ На указанное время	На указанное время
Время	На время срабатывания
Дополнительный выход №1	На время срабатывания и после срабатывания
	☐

- ✓ **На указанное время** – выбранные дополнительные выходы будут активизированы на указанное время.
 - ✓ **На время срабатывания** – выбранные дополнительные выходы будут активизированы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.
 - ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут активизированы на время, в течение которого на данном дополнительном входе будет присутствовать управляющий сигнал плюс указанное вами время.
- **Дополнительные выходы, нормализируемые при активизации.** Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализованы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть нормализованы. Кроме этого, укажите временной критерий нормализации, который может быть одним из трех видов:

☐ Критерий нормализации	На указанное время
☐ На указанное время	На указанное время
Время	На время срабатывания
Дополнительный выход №1	На время срабатывания и после срабатывания
	☐

- ✓ **На указанное время** – выбранные дополнительные выходы будут нормализованы на указанное время.
- ✓ **На время срабатывания** – выбранные дополнительные выходы будут нормализованы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.
- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут нормализованы на время, в течение которого на данном дополнительном входе будет присутствовать управляющий сигнал плюс указанное вами время.

- **Дополнительные выходы, реагирующие через группу ресурсов.** Этот параметр указывает те дополнительные выходы, которые будут активизированы, при условии, что данный дополнительный вход входит в группу ресурсов.

Тип входа – **Специальный**. Предназначен для автономного сброса тревоги в состоянии «Тревога как СКУД» либо выключения sireны в состоянии «Тревога как ОПС».

Текущее наименование	Дополнительный вход №2
Адрес	2
Первоначальное наименование	Дополнительный вход №2
Нормальное состояние контакта	Разомкнут
Тип	Специальный ▼
☐ Специальный	
Сброс тревоги (Генератор тревоги)	☐
Сброс sireны (Выход "С" ОПС)	☐

Если данный дополнительный вход используется как вход автономного сброса тревоги, укажите, какой тип тревоги, которая будет сбрасываться при поступлении управляющего сигнала на этот дополнительный вход.

Возможны два варианта:

- ✓ **Сброс тревоги (Генератор тревоги).** В этом случае при возникновении тревоги из-за ситуации, описанной в генераторе тревоги, получение управляющего сигнала на данном дополнительном входе приведет к ее сбросу.
- ✓ **Сброс sireны (Выход «С» ОПС).** Аналогично предыдущему, но будет выключена sireна, подключенная к выходу «С» ОПС.

Дополнительный выход

Каждый контроллер доступа, в зависимости от своего типа, имеет от одного до шести дополнительных выходов и один звуковой извещатель.

Дополнительные выходы могут быть использованы для управления любым внешним оборудованием в рамках системы безопасности. Технические параметры дополнительных выходов для каждого типа контроллеров приведены в техническом описании системы безопасности.

В зависимости от того, какое внешнее оборудование подключено к дополнительному выходу, существуют следующие варианты описания параметров его работы:

- При условии, что к данному дополнительному выходу не подключено никакое внешнее оборудование, менять параметры работы дополнительного выхода не нужно.
- Тип дополнительного выхода – **Обычный**.

Текущее наименование	Дополнительный выход №2
Адрес	2
Первоначальное наименование	Дополнительный выход №2
▢Тип	Обычный
▢Обычный	
Нормальное состояние	Не запитан

Этот параметр указывает, что к данному дополнительному выходу подключено внешнее оборудование, логика управления которым описывается через описание других устройств системы (за исключением генератора тревоги). Так же задайте нормальное состояние контактов для данного дополнительного выхода. Существуют два варианта – запитан/не запитан. Этот параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий.

- Тип дополнительного выхода – **Генератора тревоги**.

Текущее наименование	Дополнительный выход №3
Адрес	3
Первоначальное наименование	Дополнительный выход №3
▢Тип	Генератора тревоги ▾
▢Генератора тревоги	
Нормальное состояние	Не запитан
Время активизации	1 сек.

В этом случае решение об активизации дополнительного выхода принимается исключительно контроллером в соответствии с параметрами, указанными в его генераторе тревоги. Этот дополнительный выход будет использоваться исключительно для индикации перехода контроллера в состояние «Тревога». Так же задайте нормальное состояние контактов для данного дополнительного выхода. Существуют два варианта – запитан/не запитан. Этот параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий. Кроме этого, укажите время активизации дополнительного выхода, время, в течение которого при наличии активизирующего управляющего воздействия выход меняет своё состояние из нормализованного на противоположное. Как правило, в этом случае к такому дополнительному выходу подключают тревожный оповещатель (сирена, проблесковая лампа).

- Тип дополнительного выхода – **ОПС**.

Текущее наименование	Дополнительный выход №1
Адрес	1
Первоначальное наименование	Дополнительный выход №1
Тип	ОПС
ОПС	
Программа управления	Выключить на время при невзятии
Выключить на время при невзятии	
Время активизации	3 сек.

В этом случае дополнительный выход предназначен для управления световым оповещением (СО), звуковым оповещением (ЗО), а так же для передачи тревожных извещений на пост центрального наблюдения (ПЦН) при активизации шлейфов сигнализации (ШС), дополнительных входов или контакта ИУ, входящих в группу ресурсов.

Программа управления задает логику работы контроллера по управлению данным дополнительным выходом. Вид программы выбирается из выпадающего списка.

Возможны следующие варианты программ управления:

- ✓ **Не управлять.** Дополнительный выход не используется как элемент системы охранной сигнализации.
- ✓ **Включить при тревоге.** В случае возникновения тревоги произойдет замыкание контакта дополнительного выхода.
- ✓ **Выключить при тревоге.** В случае возникновения тревоги произойдет размыкание контакта дополнительного выхода.
- ✓ **Включить на время при тревоге.** В случае возникновения тревоги произойдет замыкание контакта дополнительного выхода на время указанное в параметре время активизации.
- ✓ **Выключить на время при тревоге.** В случае возникновения тревоги произойдет размыкание контакта дополнительного выхода на время указанное в параметре время активизации.
- ✓ **Мигать из состояния выключено при тревоге.** В этом случае в ситуации отсутствия тревоги контакты дополнительного выхода разомкнуты. В случае возникновения тревоги произойдет попеременное замыкание – размыкание контактов дополнительного выхода.
- ✓ **Мигать из состояния включено при тревоге.** В этом случае в ситуации отсутствия тревоги контакты дополнительного выхода замкнуты. В случае возникновения тревоги произойдет попеременное размыкание - замыкание контактов дополнительного выхода.
- ✓ **Мигать на время из состояния выключено при тревоге.** В этом случае в ситуации отсутствия тревоги контакты дополнительного выхода разомкнуты. В случае возникновения тревоги произойдет попеременное замыкание – размыкание контактов дополнительного выхода на время, указанное в параметре время активизации.
- ✓ **Мигать на время из состояния включено при тревоге.** В этом случае в ситуации отсутствия тревоги контакты дополнительного выхода замкнуты. В случае возникновения тревоги произойдет

- ✓ **Лампа** – программа управления, указывающая на то, что к данному дополнительному выходу подключен световой оповещатель тревожной ситуации.
- ✓ **ПЦН** – программа управления, указывающая на то, что данный дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН).
- ✓ **ПЦН (старая тактика)** – программа управления, указывающая на то, что данный дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН) по старой тактике передачи тревожного оповещения.
- ✓ **Сирена** – программа управления, указывающая на то, что к данному дополнительному выходу подключен звуковой оповещатель тревожной ситуации.
- ✓ **Включить на время перед взятием** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода на время, указанное в параметре время активизации, перед началом взятия шлейфа на охрану.
- ✓ **Выключить на время перед взятием** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода на время, указанное в параметре время активизации, перед началом взятия шлейфа на охрану.
- ✓ **Включить на время при взятии** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода на время, указанное в параметре время активизации, при взятии шлейфа на охрану.
- ✓ **Выключить на время при взятии** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода на время, указанное в параметре время активизации, при взятии шлейфа на охрану.
- ✓ **Включить при взятии** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода при взятии шлейфа на охрану.
- ✓ **Выключить при взятии** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода при взятии шлейфа на охрану.
- ✓ **Включить на время при снятии** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода на время, указанное в параметре время активизации, при снятии шлейфа с охраны.
- ✓ **Выключить на время при снятии** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода на время, указанное в параметре время активизации, при снятии шлейфа с охраны.
- ✓ **Включить при снятии** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода при снятии шлейфа с охраны.
- ✓ **Выключить при снятии** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода при снятии шлейфа с охраны.

- ✓ **Включить на время при невзятии** – программа управления, указывающая на необходимость замкнуть контакты дополнительного выхода при невозможности взятия шлейфа на охрану.
- ✓ **Выключить на время при невзятии** – программа управления, указывающая на необходимость разомкнуть контакты дополнительного выхода при невозможности взятия шлейфа на охрану.

Исполнительное устройство

Каждый контроллер управления доступом может управлять одним исполнительным устройством. Тип исполнительного устройства определяется типом контроллера. Так как контроллер не может автоматически определить параметры функционирования исполнительного устройства, задайте их. Для этого выберите исполнительное устройство у контроллера. В правой части в панели параметров будут отображены все возможные параметры функционирования.

Для контроллера управления замком:

Текущее наименование	Замок
Первоначальное наименование	Замок
Прямое направление прохода	☒
Нормальное (т.е. заблокированное) состояние контакта (вход ИУ)	Нормально замкнут
Нормальное состояние "Закрито" выхода ИУ	Не запитан
Нормализация выхода ИУ	После "Открытия"
Режим работы выхода управления ИУ	Потенциальный
Предельное время разблокировки	8 сек.
Время удержания в разблокируемом состоянии (время анализа идентификатора)	4 сек.
Регистрация прохода по предъявлению идентификатора	☐
Внутренняя защита от передачи идентификаторов (Local Antipass)	☐
Дополнительные выходы, реагирующие через группу ресурсов	
Дополнительный выход №4	☐
Дополнительный выход №5	☐

Для контроллера управления турникетом:

Текущее наименование	Турникет
Первоначальное наименование	Турникет
Прямое направление прохода	☒
Нормальное (т.е. заблокированное) состояние контакта (вход ИУ)	Нормально замкнут
Нормальное состояние "Закрито" выхода ИУ	Не запитан
Нормализация выхода ИУ	После "Открытия"
Предельное время разблокировки	8 сек.
Время удержания в разблокируемом состоянии (время анализа идентификатора)	4 сек.
Регистрация прохода по предъявлению идентификатора	☐
Внутренняя защита от передачи идентификаторов (Local Antipass)	☐

Большинство параметров идентичны для всех типов контроллеров. Отличительные особенности будут описаны ниже после описания основных параметров. Ниже приведено описание параметров исполнительного устройства:

- ✓ **Прямое направление прохода.** Данный параметр определяет, в какую сторону будет разблокирован ИУ при предъявлении карты к первому считывателю контроллера.
- ✓ **Нормальное (т.е. заблокированное) состояние контакта (вход ИУ).** Параметр описывает состояние датчика двери/турникета. В зависимости от его конструкции

он может быть при закрытом ИУ замкнут (как правило, герконы двери) или разомкнут.

- ✓ **Нормальное состояние «Закрыто» выхода ИУ.** Параметр описывает должен ли контроллер подавать напряжение на ИУ в состоянии «Закрыто». Так, например, для электромагнитных замков в состоянии «Закрыто» необходимо подавать напряжение на ИУ, для электромеханических такой необходимости нет.
- ✓ **Нормализация выхода ИУ.** Параметр описывает, в какой момент времени контроллер должен начать свои действия по блокировке ИУ (сразу после открытия ИУ или после его закрытия). Факт открытия/закрытия ИУ контроллер определяет по датчику, установленному на вход ИУ.
- ✓ **Режим работы выхода управления ИУ.** описывает логику управления подключенным исполнительным устройством. Его значение определяется исходя из параметров работы подключенного устройства.
- ✓ **Предельное время разблокировки** описывает время, по истечении которого контроллер перейдет в состояние тревога по причине того, что исполнительное устройство не заблокировано.
- ✓ **Время удержание в разблокированном состоянии** (время анализа идентификатора) описывает время, по истечении которого контроллер управления доступом переведет исполнительное устройство в состояние «Закрыто». Снимет управляющий сигнал с линии управления исполнительным устройством.
- ✓ **Регистрация прохода по предъявлению идентификатора** указывает на то, что контроллер будет считать проход совершившимся сразу после поднесения идентификатора доступа к его считывателю, игнорируя информацию о сигнале, получаемом с датчика ИУ.
- ✓ **Внутренняя защита от передачи идентификаторов** задает режим работы контроллера по контролю за повторными входами. При отмеченной опции, контроллер будет блокировать попытки повторного входа/выхода.
- ✓ **Дополнительные выходы, реагирующие через группу ресурсов.** Параметр указывает, должны ли активизироваться отмеченные дополнительные выходы, при условии, что исполнительное устройство входит в группу ресурсов.

Считыватель

В зависимости от типа используемого контроллера количество считывателей может быть от одного до двух. Так же считыватель может быть уже интегрирован в корпус контроллера.

Задание параметров функционирования считывателей фактически определяет порядок и условия работы контроллера при предъявлении идентификатора доступа. Часть параметров считывателя определяют параметры разрешения прохода в направлении, контролируемом данным считывателем.

Текущее наименование	Считыватель №1
Первоначальное наименование	Считыватель №1
Модель	PERCo-IPxx
Время ожидания подтверждения при верификации	5 сек.
=Запрещение ДУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	☐
в РЕЖИМЕ РАБОТЫ "Совещание"	☐
=Подтверждение от ДУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
=Защита от передачи идентификаторов (Antipass)	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
в РЕЖИМЕ РАБОТЫ "Охрана"	Нет
+Дополнительные входы, маскируемые при разблокировке ИУ	
+Дополнительные выходы, активизируемые при разблокировке ИУ	
+Дополнительные выходы, нормализируемые при разблокировке ИУ	
+Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов сотрудников	

- ✓ **Время ожидания подтверждения при верификации** - временной параметр, который устанавливает время, в течение которого контроллер будет ожидать поднесения коммиссионированного идентификатора или подтверждения от верифицирующего устройства. В качестве верифицирующего устройства может быть использовано ДУ контроллера или программное обеспечение.
- ✓ **Запрещение ДУ** - параметр, который дает возможность запретить работу ДУ контроллера по разблокировке ИУ в направлении работы данного считывателя в выбранных режимах доступа. При установке данного параметра произвести разблокировку ИУ в этом направлении в выбранных режимах доступа будет невозможно.
- ✓ **Подтверждение от ДУ**. При помощи этого параметра можно указать как в выбранных режимах доступа при поднесении идентификатора к данному считывателю будет формироваться запрос на подтверждение от ДУ.

=Подтверждение от ДУ	
☐ в РЕЖИМЕ РАБОТЫ "Контроль"	Да
☐ Да	
☐ Верифицировать идентификаторы Сотрудников	
при проходе	☐
при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ	☐
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет

- ✓ Можно гибко настроить условия верификации идентификаторов сотрудников/учеников. Имеются следующие условия верификации:
 - ✓ **при проходе** — верификация будет осуществляется при попытке прохода без каких-либо нарушений
 - ✓ **при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ** — верификация будет осуществляется случае попытки повторного прохода без предварительного прохода в обратную сторону (параметр «Защита от передачи идентификаторов» должен быть установлен на значение «Мягкая или Жесткая»)

- ✓ **Защита от передачи идентификаторов** - параметр, который позволяет определить реакцию контроллера в случае попытки повторного прохода без предварительного прохода в обратную сторону. Для каждого из указанных режимов работы контроллера можно выбрать один из вариантов работы:

- ✓ **Нет.** Контроллер не осуществляет проверку факта повторного прохода по идентификатору, предъявленному к выбранному считывателю.
- ✓ **Мягкая.** Контроллер разрешит повторный проход по идентификатору, предъявленному к выбранному считывателю и при этом в журнале регистрации записывается событие о проходе с нарушением зональности.
- ✓ **Жесткая.** Контроллер запретит попытку повторного прохода при предъявлении идентификатора к выбранному считывателю и при этом в журнал регистрации записывается событие о запрете прохода по причине нарушения зональности, а в журнале мониторинга — событие о предъявлении такого идентификатора.

Кроме перечисленных выше параметров можно указать дополнительные параметры, влияющие на действия контроллера при поднесении идентификатора:

Дополнительные входы, маскируемые при разблокировке ИУ	
☐ Критерий маскирования	На указанное время
☐ На указанное время	
Время	3 сек.
Дополнительный вход №1	☐
Дополнительный вход №2	☐
Дополнительные выходы, активизируемые при разблокировке ИУ	
Критерий активизации	На время срабатывания
Дополнительный выход №1	☐
Дополнительный выход №2	☐
Дополнительные выходы, нормализируемые при разблокировке ИУ	
☐ Критерий нормализации	На время срабатывания и после срабатывания
☐ На время срабатывания и после срабатывания	
Время	250 мс.
Дополнительный выход №1	☐
Дополнительный выход №2	☐
Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов сотрудников	
☐ Критерий активизации	На указанное время
☐ На указанное время	
Время	3 сек.
Дополнительный выход №1	☐
Дополнительный выход №2	☐

- ✓ **Дополнительные входы, маскируемые при разблокировке ИУ.** Этот параметр позволяет указать, какие именно дополнительные входы контроллера должны быть маскированы, т.е. не воспринимать управляющий сигнал от внешнего оборудования, при разблокировке ИУ. Для выбора отметьте флажки тех дополнительных входов, которые должны быть маскированы. Кроме этого, укажите временной критерий маскирования, который может быть одним из трех видов:

Критерий маскирования	На указанное время
На указанное время	На указанное время
Время	На время срабатывания
Дополнительный вход №2	На время срабатывания и после срабатывания

- ✓ **На указанное время** – выбранные дополнительные входы будут маскированы на указанное время.
- ✓ **На время срабатывания** – выбранные дополнительные входы будут маскированы на протяжении всего времени, когда ИУ будет разблокировано.
- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные входы будут маскированы на время, в течение которого ИУ будет разблокировано плюс указанное вами время.
- ✓ **Дополнительные выходы, активизируемые при разблокировке ИУ.** Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть активизированы при разблокировке ИУ. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть активизированы. Кроме этого, укажите временной критерий активизации, который может быть одним из трех видов:

Критерий активизации	На указанное время
На указанное время	На указанное время
Время	На время срабатывания
Дополнительный выход №1	На время срабатывания и после срабатывания

- ✓ **На указанное время** – выбранные дополнительные выходы будут активизированы на указанное время.
- ✓ **На время срабатывания** – выбранные дополнительные выходы будут активизированы на протяжении всего времени, когда ИУ будет разблокировано.
- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут активизированы на время, в течение которого ИУ будет разблокировано плюс указанное вами время.
- ✓ **Дополнительные выходы, нормализуемые при разблокировке ИУ.** Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализованы при разблокировке ИУ. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть нормализованы. Кроме этого, укажите временной критерий нормализации, который может быть одним из трех видов:

Критерий нормализации	На указанное время
На указанное время	На указанное время
Время	На время срабатывания
Дополнительный выход №1	На время срабатывания и после срабатывания

- ✓ **На указанное время** – выбранные дополнительные выходы будут нормализованы на указанное время.
- ✓ **На время срабатывания** – выбранные дополнительные выходы будут нормализованы на протяжении всего времени, когда ИУ будет разблокировано.

- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут нормализованы на время, в течение которого ИУ будет разблокировано плюс указанное вами время.
- ✓ **Дополнительные выходы, активизируемые при предъявлении валидных пропусков сотрудников.** Этот параметр позволяет указать те дополнительные выходы, которые будут активизированы на указанное время в случае предъявления не заблокированного и с не истёкшим сроком действия идентификатора сотрудника/ученика. Этот параметр может быть использован в случае, если к этим дополнительным выходам подключена дополнительная индикация, информирующая работников охраны о статусе предъявленной карты. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть активизированы. Кроме этого, укажите временной критерий активизации, который может быть одним из трех видов:

☐ Критерий активизации	На указанное время
☐ На указанное время	На указанное время
Время	На время срабатывания
Дополнительный выход №1	На время срабатывания и после срабатывания

- ✓ **На указанное время** – выбранные дополнительные выходы будут активизированы на указанное время начиная с момента предъявления идентификатора, независимо от того будет или нет разрешён проход.
- ✓ **На время срабатывания** – выбранные дополнительные выходы будут активизированы на указанное время начиная с момента разблокирования ИУ и до момента его заблокирования, либо, если проход не был совершён, по истечению времени анализа идентификатора.
- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут активизированы на указанное время начиная с момента разблокирования ИУ и до момента его заблокирования плюс указанное вами время, либо, если проход не был совершён, по истечению времени анализа идентификатора.

Генератор тревоги

В зависимости от структуры системы безопасности, ее задач, местоположения контроллера управления доступом, текущего режима доступа те или иные действия пользователей системы могут приводить к генерации тревоги.

Для выявления причин генерации тревоги и управления выделенным выходом тревоги (один из дополнительных выходов) определите следующие параметры:

Текущее наименование	Генератор тревоги
Первоначальное наименование	Генератор тревоги
Генерация тревоги при предъявлении идентификатора	
если ИДЕНТИФИКАТОР НЕ ЗАРЕГИСТРИРОВАН	Нет
если ИДЕНТИФИКАТОР ЗАПРЕЩЕН	Нет
если ИДЕНТИФИКАТОР ИЗ СТОП-ЛИСТА	Нет
если ИСТЕК СРОК ДЕЙСТВИЯ	Нет
если НАРУШЕНО ВРЕМЯ	Нет
если НАРУШЕНА ЗОНАЛЬНОСТЬ	Нет
если НАРУШЕН РЕЖИМ РАБОТЫ	Нет
если НАРУШЕНО КОМИССИОНИРОВАНИЕ	Нет
Генерация тревоги при несанкционированной разблокировке ИУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
в РЕЖИМЕ РАБОТЫ "Закрыто"	Нет
Генерация тревоги по недопустимо долгому открытию ИУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
Генерация тревоги по датчику вскрытия корпуса контроллера	Нет
Дополнительные входы, активизирующие генерацию тревоги	
Тип тревоги	Тихая
Дополнительный вход №1	☐
Дополнительный вход №2	☐

- ✓ **Генерация тревоги при предъявлении идентификатора.** Этот параметр позволяет указать причины генерации тревожных событие и перехода контроллера в состояние «Тревога» при предъявлении идентификатора с указанными параметрами доступа.
- ✓ **Генерация тревоги при несанкционированной разблокировке ИУ.** Этот параметр позволяет указать, будет ли контроллер автоматически генерировать тревожное событие и переходить в состояние «Тревога» в случае разблокировки ИУ при помощи ключа (то есть разблокировке ИУ без команды от контроллера) в выбранных режимах доступа.
- ✓ **Генерация тревоги по недопустимо долгому открытию ИУ.** Этот параметр позволяет указать, будет ли контроллер автоматически генерировать тревожное событие и переходить в состояние «Тревога» в случае, если после открытия ИУ оно не было приведено в исходное состояние в течение времени большего, чем указано в параметрах этого ИУ. Другими словами, должен ли контроллер перейти в состояние «Тревога», если после прохода через дверь она осталось открытой.
- ✓ **Дополнительные входы, активизирующие генерацию тревоги** – параметр, позволяющий выбрать те дополнительные входы контроллера, активизация которых будет приводить к переходу контроллера в состояние «Тревога». Это может быть использовано, например, при подключении к этому дополнительному входу кнопки тревожной сигнализации.
- ✓ **Тип тревоги** – параметр, который позволяет управлять активизацией дополнительного выхода контроллера, помеченного как «Выход генерации тревоги». Имеются два возможных значения:

Тихая
Тихая
Громкая

- ✓ Тихая — в этом случае активизация дополнительного выхода не произойдет, а контроллер запишет в журнал регистрации и в журнал мониторинга событие о тревоге
- ✓ Громкая - в этом случае произойдет активизация дополнительного выхода и контроллер запишет в журнал регистрации и в журнал мониторинга событие о тревоге

Шлейф сигнализации

Контроллеры имеют возможность подключения стандартных шлейфов охранной сигнализации. Использование охранного шлейфа позволяет системе безопасности контролировать не только вход в помещение, но и внутренний объем помещения, открывание окон и так далее за счет подключения дополнительных охранных датчиков.

Для задания параметров работы шлейфа сигнализации выберите в дереве объектов интересующий шлейф сигнализации. В панели параметров отобразятся его параметры функционирования:

Текущее наименование	Шлейф сигнализации №1
Первоначальное наименование	Шлейф сигнализации №1
Тип	Охранный
Автоматическое перевзятие	☒
Тихая тревога	☒
Повторное включение сирены	☐
Длительность нарушения	70 мс.
Задержка взятия на охрану	0 мс.
Задержка управления выходом "С"	0 мс.
Задержка управления выходом "Л"	0 мс.
Задержка восстановления нарушенного шлейфа в снятом состоянии	0 мс.
Дополнительные выходы, реагирующие через группу ресурсов	
Дополнительный выход №4	☐
Дополнительный выход №5	☐

- ✓ **Тип.** Параметр дает возможность указать тип шлейфа охранной сигнализации, определяемый типом подключаемых к нему охранных датчиков:

Охранный
Охранный
Охранный с контролем блокировки

- ✓ **Охранный**
- ✓ **Охранный с контролем блокировки**
- ✓ **Автоматическое перевзятие.** При включенной опции, при постановке на охрану шлейфа охранной сигнализации, в случае невозможности взятия шлейфа на охрану, контроллер автоматически будет пытаться взять шлейф на охрану повторно.

- ✓ **Тихая тревога.** При включении этой опции, если в состав шлейфа включены дополнительные выходы, работающие по программам «Сирена» или «Лампа», то эти программы не будут активизированы.
- ✓ **Повторное включение сирены.** Параметр указывает, должен ли контроллер повторно включить сирену, при условии повторного нарушения шлейфа.
- ✓ **Длительность нарушения.** Параметр указывает временной параметр, в течении которого нарушение шлейфа не будет считаться тревожным.
- ✓ **Задержка взятия на охрану** – интервал времени, по истечении которого контроллер начнет анализировать состояние шлейфа охранной сигнализации для постановки на охрану. Как правило, это время устанавливают отличным от нуля в ситуации, когда место постановки на охрану находится под контролем этого шлейфа. И после постановки на охрану необходимо время для того, чтобы покинуть охраняемое помещение.
- ✓ **Задержка управления выходом «С».** Параметр указывает время в течении которого контроллер не будет активизировать выход с программой управления «Сирена» после нарушения шлейфа.
- ✓ **Задержка управления выходом «Л».** Параметр указывает время в течении которого контроллер не будет активизировать выход с программой управления «Лампа» после нарушения шлейфа.
- ✓ **Задержка восстановления нарушенного шлейфа в снятом состоянии.** Параметр указывает время, по истечении которого контроллер будет пытаться восстановить нарушенный шлейф. Если значение параметра установлено 0 или Бесконечность, а шлейф находится в снятом состоянии - сопротивление шлейфа не отслеживается.
- ✓ **Дополнительные выходы.** Вы можете указать дополнительные выходы этого контроллера, состояние которых будет меняться по заданной программе в зависимости от состояния данного шлейфа.



ПРИМЕЧАНИЕ

Могут быть задействованы только дополнительные выходы, у которых в качестве типа указан тип «ОПС».

Группы ресурсов

Группа ресурсов – логическая структура, которая позволяет создать комбинации ресурсов контроллера, которые будут ставиться на охрану в зависимости от прав пользователя системы.

Для добавления группы ресурсов выделите группу ресурсов интересующего контроллера и щелкните на кнопке . В дереве объектов выделенного контроллера появятся дополнительная группа ресурсов. Выбрав ее, можно задать следующие параметры:

Текущее наименование	Группа ресурсов №1
Первоначальное наименование	Группа ресурсов №1
Включить ИУ в группу	☒
[-] <u>Дополнительные входы, включённые в группу</u>	
Дополнительный вход №1	☐
Дополнительный вход №2	☐
[-] <u>Шлейфы сигнализации, включённые в группу</u>	
Шлейф сигнализации №1	☐
Шлейф сигнализации №2	☐

- ✓ **Включить ИУ в группу** – параметр, указывающий на то, входит ли исполнительное устройство в эту группу. То есть, если исполнительное устройство добавлено в группу, при постановке на охрану контроллер будет контролировать его состояние. В противном случае открытие двери не будет приводить к возникновению тревоги после постановки группы ресурсов на охрану. Это может быть использовано в том случае, когда ресурсы контроллера используются не только для контроля помещения, доступ в которое он контролирует.
- ✓ **Дополнительные входы, входящие в группу.** Параметр позволяет указать дополнительные входы контроллера, которые будут контролироваться контроллером при постановке группы ресурсов на охрану.
- ✓ **Шлейфы сигнализации, входящие в группу.** Параметр позволяет указать, шлейфы сигнализации, которые будут контролироваться контроллером при постановке группы ресурсов на охрану.

Защита от передачи идентификаторов

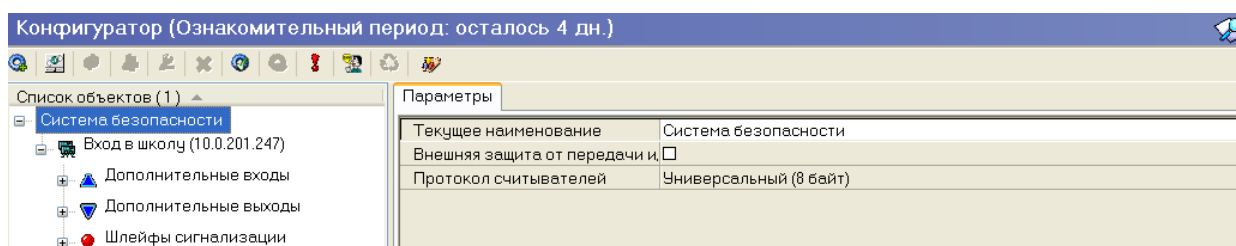
Контроллеры доступа поддерживают режим *защиты от передачи идентификаторов*, т.е. запрет повторного входа без предварительного выхода.

Для реализации этого режима, факт прохода с данной картой передается другим контроллерам сети. Так как при конфигурации контроллеров (см. «[Конфигурация контроллеров](#)») каждому контроллеру передаются списки контроллеров других подсетей, то алгоритм передачи следующий:

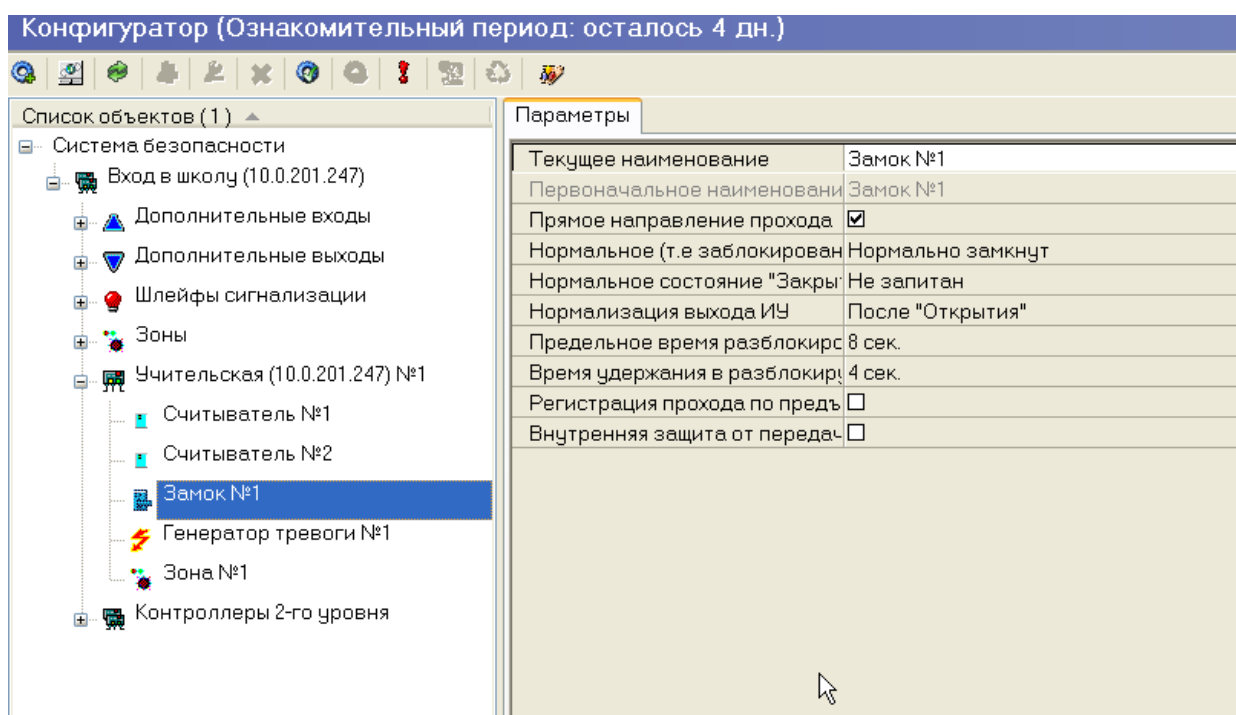
- ✓ Происходит широковещательная рассылка контроллерам своей подсети.
- ✓ Выбирается первый контроллер другой подсети, и ему передаются данные. В случае невозможности передачи ему, выбирается следующий контроллер этой подсети и т.д. Затем эта же процедура проводится и с другими подсетями.
- ✓ Контроллер в другой подсети, получив данные, распространяет их широковещательно по всем контроллерам своей подсети.
- ✓ В результате этих действий каждый контроллер знает, на каком из уровней доступа (безопасности) находится владелец предъявленной карты.

По умолчанию все идентификаторы, зарегистрированные в системе безопасности контролируются на предмет повторного входа/выхода. Для включения защиты от передачи идентификаторов в разделе Конфигуратор:

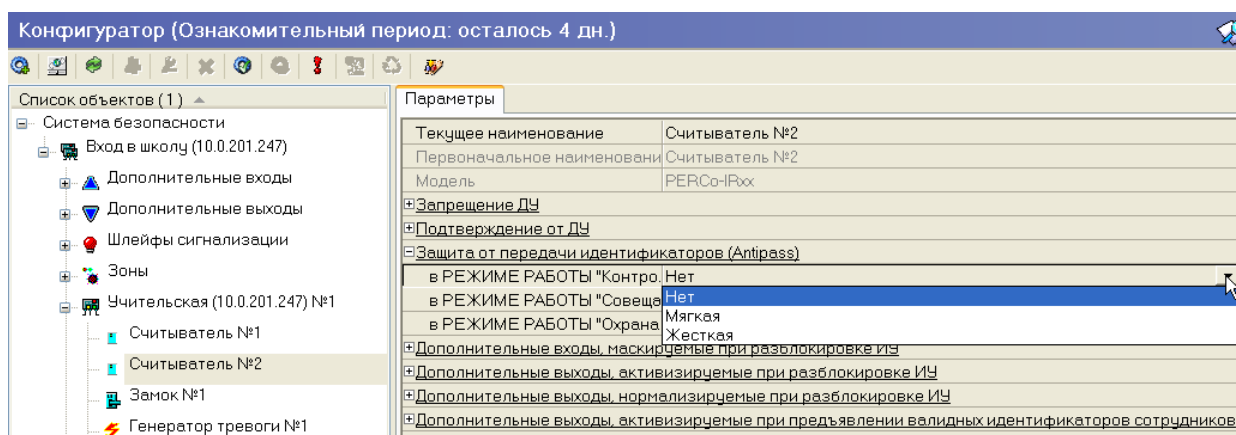
- ✓ для системы безопасности в целом: отметьте флажок **Внешняя защита от передачи идентификаторов (Global Antipass)** в панели параметров



- ✓ для отдельного исполнительного устройства: отметьте флажок **Внутренняя защита от передачи идентификаторов (Local Antipass)** в панели параметров

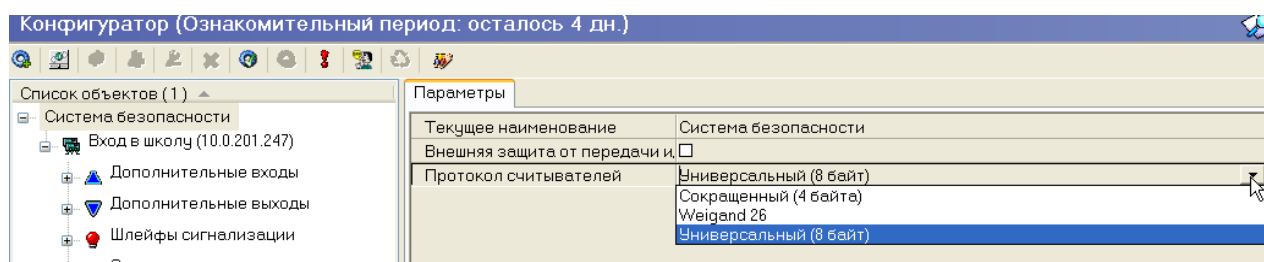


- ✓ для отдельного считывателя: установите у считывателя в параметре **Защита от передачи идентификаторов (Antipass)** значение **Жесткая**: для требуемых режимов работы



Протокол работы со считывателями

Контроллеры доступа поддерживают три формата получения данных от считывателей. Для изменения протокола в разделе *Конфигуратор* измените параметр «Протокол считывателей».



Имеется три значения этого параметра:

- **Универсальный (8 байт)** — формат данных, по которому контроллер воспринимает 64 бита кода идентификатора доступа
- **Widgand 26** – формат данных, по которому контроллер воспринимает 24 бита кода идентификатора доступа
- **Сокращённый (4 байта)** — формат данных, по которому контроллер воспринимает 32 бита кода идентификатора доступа

Описание параметров функционирования контроллеров КБО (серия CS01)

Подробная информация о параметрах функционирования контроллера КБО приведена в техническом описании системы безопасности.

Контроллер КБО предназначен для контроля состояния шлейфов сигнализации (ШС), пожарных или охранных, выдачи тревожных сообщений на пост центрального наблюдения (ПЦН), световое оповещение (СО) и звуковое оповещение (ЗО), управления дополнительным оборудованием, сохранению событий, произошедших в системе, в энергонезависимой памяти и передаче их ПО. Дополнительно панель КБО обеспечивает управление одним электромагнитным или электромеханическим замком.

Ниже будут приведены общие рекомендации, проиллюстрированные примерами задания параметров ресурсов контроллеров.

Контроллер

Каждый контроллер имеет следующие параметры:

Использовать встроенный звуковой извещатель	☐
Режим активизации кнопки "КЛЮЧ"	Одно длинное нажатие ▼
	Одно нажатие
	Одно длинное нажатие
	Два длинных нажатия
	Три коротких нажатия

- **Использовать встроенный звуковой извещатель** — параметр, управляющий звуковой индикацией на блоке управления индикацией (БУИ). При сбросе данного параметра встроенный звуковой индикатор у БУИ будет включаться только по части СКУД. На контроллере будет действовать только световая индикация.
- **Режим активизации кнопки "КЛЮЧ"** — параметр, задающий способ разблокирования управления на блоке управления индикацией (БУИ). Имеются следующие значения:

- ✓ **Одно нажатие**
- ✓ **Одно длинное нажатие**
- ✓ **Два длинных нажатия**
- ✓ **Три коротких нажатия**

Дополнительный выход

Каждый контроллер имеет шесть дополнительных выходов (первый выход зарезервирован).

Дополнительные выходы могут быть использованы для управления любым дополнительным оборудованием в рамках системы безопасности. Технические параметры дополнительных выходов для каждого типа контроллера приведены в техническом описании системы безопасности.

В зависимости от алгоритма работы внешних устройств, подключенных к дополнительному выходу существуют следующие варианты описания параметров работы выхода:

- ✓ При условии, что к данному дополнительному выходу не подключено никакое дополнительное оборудование, менять параметры работы выхода не нужно.
- ✓ Тип дополнительного выхода – **Обычный**

Текущее наименование	Дополнительный выход №2
Адрес	2
Первоначальное наименование	Дополнительный выход №2
≡ Тип	Обычный ▾
≡ Обычный	
Нормальное состояние	Не запитан

Этот параметр указывает, что к данному дополнительному выходу подключено дополнительное оборудование, логика управления которым описывается через описание других устройств системы (за исключением генератора тревоги). Задайте нормальное состояние контактов для данного дополнительного выхода. Существуют два варианта – запитан/незапитан. Этот параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий.

- ✓ Тип дополнительного выхода – **генератора тревоги**.

Текущее наименование	Дополнительный выход №3
Адрес	3
Первоначальное наименование	Дополнительный выход №3
Тип	Генератора тревоги
Генератора тревоги	
Нормальное состояние	Не запитан
Время активизации	1 сек.

В этом случае решение об активизации дополнительного выхода принимается исключительно панелью в соответствии с параметрами, указанными в ее генераторе тревоги. Этот дополнительный выход будет использоваться для индикации перехода панели в состояние «Тревога». Так же задайте нормальное состояние контактов для данного дополнительного выхода. Существуют два варианта – запитан/не запитан. Этот параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий. Кроме этого, укажите время активизации дополнительного выхода, время, в течение которого при наличии активизирующего управляющего воздействия выход меняет своё состояние из нормализованного на противоположное. Как правило, в этом случае к такому дополнительному выходу подключают тревожный оповещатель (сирена, проблесковая лампа).

✓ Тип дополнительного выхода – **ОПС**.

Текущее наименование	Дополнительный выход №2
Адрес	2
Первоначальное наименование	Дополнительный выход №2
Тип	ОПС
ОПС	
Нормальное состояние	Не запитан
Задержка перед запуском	0 мс.
Время активизации	1 сек.
Программа управления	Включить при пожаре
Зоны, активизирующие выход	
Охранная зона	☐
Пожарная зона	☐

В этом случае дополнительный выход предназначен для управления световым оповещением (СО), звуковым оповещением (ЗО), а так же для передачи тревожных извещений на пульт центрального наблюдения (ПЦН) при изменении режимов и состояний пожарной зоны (ПЗ) и охранной зоны (ОЗ).

Программа управления задает логику работы панели по управлению этим дополнительным выходом. Инициатором активизации выхода являются изменения режимов и состояний зон, отмеченных под параметром «Зоны, активизирующие выход». После возникновения события, инициирующего активизацию выхода (в соответствии с заданной программой), начинается отсчёт задержки, указанной в параметре «Задержка перед запуском» (если задержка ненулевая), по окончании которой выход активизируется. В зависимости от программы управления выход может быть запитан (не запитан) постоянно (пока ресурс панели находится в текущем режиме), либо изменять своё физическое состояние (мигать) из нормализованного на противоположное.

Нормализация выхода происходит либо по истечению времени, указанному в параметре «Время активизации» (если оно не бесконечное), либо по сбросу панели, либо после выключения ее питания. После включения питания все выходы нормализуются.

Вид программы выбирается из выпадающего списка. Возможны следующие варианты программ управления дополнительным выходом:

- ✓ **Включить при пожаре.** В случае перехода одной из зон в режим «ПОЖАР» произойдет замыкание контакта дополнительного выхода.
- ✓ **Мигать при пожаре.** В случае перехода одной из зон в режим «ПОЖАР» произойдет попеременное размыкание - замыкание контактов дополнительного выхода.
- ✓ **Включить при внимании и пожаре.** В случае перехода одной из зон в режим «ВНИМАНИЕ» или «ПОЖАР» произойдет замыкание контакта дополнительного выхода.
- ✓ **Мигать при внимании и пожаре.** В случае перехода одной из зон в режим «ВНИМАНИЕ» или «ПОЖАР» произойдет попеременное размыкание - замыкание контактов дополнительного выхода.
- ✓ **Включить при тревоге.** В случае перехода одной из зон в режим «ТРЕВОГА» произойдет замыкание контакта дополнительного выхода.
- ✓ **Мигать при тревоге.** В случае перехода одной из зон в режим «ТРЕВОГА» произойдет попеременное размыкание - замыкание контактов дополнительного выхода.
- ✓ **Лампа 1** – программа управления, указывающая на то, что к дополнительному выходу подключен световой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы все зоны изменили свой режим.
- ✓ **Лампа 2** – программа управления, указывающая на то, что к дополнительному выходу подключен световой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы хотя бы одна из зон изменила свой режим.
- ✓ **ПЦН 1** – программа управления, указывающая на то, что дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН). Для активизации программы требуется, чтобы все зоны изменили свой режим.
- ✓ **ПЦН 2** – программа управления, указывающая на то, что дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН). Для активизации программы требуется, чтобы все зоны изменили свой режим.
- ✓ **Сирена** – программа управления, указывающая на то, что к дополнительному выходу подключен звуковой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы хотя бы одна из зон изменила свой режим.
- ✓ **Включить перед взятием** – Перед переходом одной из зон в режим «ВЗЯТИЕ» произойдет замыкание контакта дополнительного выхода.
- ✓ **Включить при взятии** — При переходе одной из зон в режим «ВЗЯТИЕ» произойдет замыкание контакта дополнительного выхода.
- ✓ **Включить при снятии** – Перед переходом одной из зон в режим «СНЯТА» произойдет замыкание контакта дополнительного выхода.
- ✓ **Включить при автоперевзятии** – При переходе одной из охранных зон в режим «АВТОПЕРЕВЗЯТИЕ» произойдет замыкание контакта дополнительного выхода.
- ✓ **Включить при неисправности.** При переходе одной из зон в режим «НЕИСПРАВНОСТЬ» произойдет замыкание контакта дополнительного выхода.

- ✓ **Мигать при неисправности.** При переходе одной из зон в режим «НЕИСПРАВНОСТЬ» произойдет попеременное размыкание - замыкание контактов дополнительного выхода.

Шлейф сигнализации

Контроллеры имеют возможность подключения стандартных шлейфов охранной и пожарной сигнализации. Использование охранных шлейфов позволяет системе безопасности контролировать не только вход в помещение, но и внутренний объем помещения, открывание окон и так далее за счет подключения дополнительных охранных датчиков. Использование пожарных шлейфов позволяет контролировать пожарную безопасность помещения за счет подключения пожарных извещателей. Имеется 3 шлейфа.

В зависимости от алгоритма работы внешних датчиков и извещателей, подключенных к шлейфу сигнализации существуют следующие варианты описания параметров работы шлейфа:

- ✓ Тип шлейфа сигнализации — **Охранный**

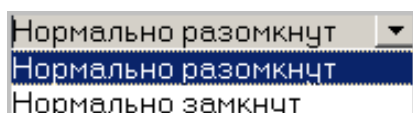
Текущее наименование	Шлейф сигнализации №1
Адрес	1
Первоначальное наименование	Шлейф сигнализации №1
Тип	Охранный
Охранный	
Контроль вскрытия корпуса извещателей	☐
Длительность нарушения	70 мс.
Задержка взятия на охрану	0 мс.
Задержка восстановления нарушенного шлейфа в снятом состоянии	0 мс.

- ✓ **Контроль вскрытия корпуса извещателей** — параметр, указывающий шлейфу контролировать вскрытие корпуса извещателей.
- ✓ **Длительность нарушения** - параметр, определяющий для шлейфа время интегрирования
- ✓ **Задержка взятия на охрану** — параметр, определяющий для шлейфа время, через которое панель предпринимает попытку взять шлейф на охрану после поступления соответствующей команды.
- ✓ **Задержка восстановления нарушенного шлейфа в снятом состоянии** — если данный параметр установлена в 0, то шлейф в состоянии «СНЯТ» не контролируется. В противном случае продолжается отслеживание шлейфа в режиме «Снят». Если при этом шлейф перейдет в состояние «НАРУШЕНИЕ», то в журнал регистраций записывается событие «Неисправность снятого ОШС», состояние выходов и встроенная звуковая индикация панели не изменяются. Если после этого нормальное состояние шлейфа восстановится и продержится время, указанное в этом параметре, то шлейф выйдет из состояния «НАРУШЕНИЕ» и при этом в журнал регистраций будет записано сообщение «Нормализация снятого ОШС». Состояние выходов и встроенная звуковая индикация панели не изменяются.

✓ Тип шлейфа сигнализации — **Пожарный**

Текущее наименование	Шлейф сигнализации №2
Адрес	2
Первоначальное наименование	Шлейф сигнализации №2
Тип	Пожарный
Нормальное состояние контактов извещателей	Нормально разомкнут
Поддержка перезапроса	☐
Задержка при включении	0 мс.
Задержка сброса	0 мс.

- ✓ **Нормальное состояние контактов извещателей** - параметр, определяющий изначальное состояние контакта извещателей, подключенных к шлейфу. Возможны два значения — нормально разомкнут или нормально замкнут.



- **Поддержка перезапроса** - параметр, определяющий, надо или нет после срабатывания извещателей снимать питание с шлейфа и перепроверять его состояние.
- **Задержка при включении** — параметр, определяющий время задержки до начала измерений сопротивления шлейфа после подачи на него питания при перезапросе и взятии.
- **Задержка сброса** — параметр, определяющий время нахождения шлейфа в состоянии «СБРОС» (без питания).

Зоны сигнализации

Зона сигнализации — это часть территории объекта, на которой физически расположены один или несколько шлейфов сигнализации. Пересечение границы охранной зоны (ОЗ) приводит к нарушению охранного шлейфа сигнализации (ОШС), входящего в данную зону, а возникновение пожарного фактора в пожарной зоне (ПЗ) (задымление, превышение определённого порога температуры, открытое пламя и т.д.) приводит к изменению состояния входящего в данную пожарную зону (ПЗ) пожарного шлейфа сигнализации (ПШС). Имеется 2 зоны, пожарная и охранная.

В зависимости от алгоритма работы шлейфов сигнализации существуют следующие варианты описания параметров работы зоны:

✓ **Тип зоны сигнализации** — Охранная

Текущее наименование	Охранная зона
Адрес	1
Первоначальное наименование	Охранная зона
Тип	Охранная
Охранная	
Повторное включение sireны	☐
Режим работы при невзятии	Тревога
Не активизировать при тревоге по Охранным шлейфам сигнализации	
Выходы, работающие по программе "Сирена" или "Лампа"	☐
Шлейфы, включенные в зону	
Шлейф сигнализации №1	☐

- ✓ **Повторное включение sireны** - параметр, позволяющий реализовать тактику активизации дополнительного выхода, управляемого по программе "Сирена" при каждом нарушении охранной зоны, даже если она уже находится в режиме "Тревога".
- ✓ **Режим работы при невзятии** — параметр указывает действие, которое будет происходить при невозможности взятия данной зоны на охрану. Имеются следующие значения:

Тревога	▼
Тревога	
Автоматическое перевзятие	
Возврат в "СНЯТ"	

- **Тревога** — зона будет переведена в режим «ТРЕВОГА».
 - **Автоматическое перевзятие** — зона будет переведена в режим «Взятие», а затем, будет производится повторная попытка взятия до тех пор, пока взятие не произойдет.
 - **Возврат в режим снят** — зона перейдет в режим «СНЯТА».
- ✓ **Не активизировать при тревоге по охранным шлейфам сигнализации дополнительные выходы, работающие по программе «Сирена» или «Лампа»** - параметр указывает, должна ли панель в случае тревоги в данной зоне запрещать активизацию дополнительных выходов, работающие по программе управления «Сирена» или «Лампа».
 - ✓ **Шлейфы, включенные в зону** - список охранных шлейфов, контролируемых в данной зоне.

- ✓ **Тип зоны сигнализации** - Пожарная

Текущее наименование	Пожарная зона
Адрес	2
Первоначальное наименование	Пожарная зона
Тип	Пожарная
Пожарная	
Количество сработавших извещателей для перехода в режим "ПОЖАР"	2
Повторное включение sireны	☐
Переводить ИЧ в режим "Открыто"	Никогда
Шлейфы, включенные в зону	
Шлейф сигнализации №2	☐

- ✓ **Количество сработавших извещателей для перехода в режим "ПОЖАР"** - параметр, задающий минимальное количество извещателей, срабатывание которых переводит данную пожарную зону в режим «ПОЖАР».
- ✓ **Переводить ИУ в режим «Открыто»** - параметр, задающий условия перевода ИУ в режим «ОТКРЫТО». Можно установить следующие значения:
 - **Никогда** — изменения режимов зон не влияют на ИУ.
 - **При переходе ПЗ в режим "ПОЖАР", но ОЗ не в режиме "Охрана"**
 - **При переходе ПЗ в режим "ПОЖАР", ОЗ в любом режиме**
 - **При переходе ПЗ в режим "ПОЖАР" или "ВНИМАНИЕ", но ОЗ не в режиме "Охрана"**
 - **При переходе ПЗ в режим "ПОЖАР" или "ВНИМАНИЕ", ОЗ в любом режиме**
 - **При переходе ПЗ в режим "ПОЖАР" (ОЗ в любом режиме) или "ВНИМАНИЕ" (ОЗ не в режиме "Охрана")**
- ✓ **Шлейфы, включенные в зону** - список пожарных шлейфов, контролируемых в данной зоне.

Исполнительное устройство

Каждый контроллер может управлять одним исполнительным устройством - замком. Так как контроллер не может автоматически определить параметры функционирования исполнительного устройства, задайте их. Для этого выберите исполнительное устройство у контроллера. В правой части в панели параметров будут отображены все возможные параметры функционирования.

Текущее наименование	Замок
Первоначальное наименование	Замок
Прямое направление прохода	☒
Нормальное (т.е. заблокированное) состояние контакта (вход ИУ)	Нормально замкнут
Нормальное состояние "Закрыто" выхода ИУ	Не запитан
Нормализация выхода ИУ	После "Открытия"
Режим работы выхода управления ИУ	Потенциальный
Предельное время разблокировки	8 сек.
Время удержания в разблокируемом состоянии (время анализа идентификатора)	4 сек.
Регистрация прохода по предъявлению идентификатора	☐
Внутренняя защита от передачи идентификаторов (Local Antipass)	☐

Ниже приведено описание параметров исполнительного устройства:

- ✓ **Прямое направление прохода.** Данный параметр определяет, в какую сторону будет разблокирован ИУ при предъявлении карты к первому считывателю контроллера.
- ✓ **Нормальное (т.е. заблокированное) состояние контакта (вход ИУ).** Параметр описывает состояние датчика двери/турникета. В зависимости от его конструкции он может быть при закрытом ИУ замкнут (как правило, герконы двери) или разомкнут.
- ✓ **Нормальное состояние «Закрыто» выхода ИУ.** Параметр описывает должен ли контроллер подавать напряжение на ИУ в состоянии «Закрыто». Так, например,

для электромагнитных замков в состоянии «Закрыто» необходимо подавать напряжение на ИУ, для электромеханических такой необходимости нет.

- ✓ **Нормализация выхода ИУ.** Параметр описывает, в какой момент времени контроллер должен начать свои действия по блокировке ИУ (сразу после открытия ИУ или после его закрытия). Факт открытия/закрытия ИУ контроллер определяет по датчику, установленному на вход ИУ.
- ✓ **Режим работы выхода управления ИУ.** описывает логику управления подключенным исполнительным устройством. Его значение определяется исходя из параметров работы подключенного устройства.
- ✓ **Предельное время разблокировки** описывает время, по истечении которого контроллер перейдет в состояние тревога по причине того, что исполнительное устройство не заблокировано.
- ✓ **Время удержание в разблокированном состоянии** (время анализа идентификатора) описывает время, по истечении которого контроллер управления доступом переведет исполнительное устройство в состояние «Закрыто». Снимет управляющий сигнал с линии управления исполнительным устройством.
- ✓ **Регистрация прохода по предъявлению идентификатора** указывает на то, что контроллер будет считать проход совершившимся сразу после поднесения идентификатора доступа к его считывателю, игнорируя информацию о сигнале, получаемом с датчика ИУ.
- ✓ **Внутренняя защита от передачи идентификаторов** задает режим работы контроллера по контролю за повторными входами. При отмеченной опции, контроллер будет блокировать попытки повторного входа/выхода.

Считыватель

Каждый контроллер поддерживает один считыватель.

Задание параметров функционирования считывателя фактически определяет порядок и условия работы контроллера при предъявлении идентификатора доступа. Часть параметров считывателя определяют параметры разрешения прохода в направлении, контролируемом данным считывателем.

Текущее наименование	Считыватель №1
Первоначальное наименование	Считыватель №1
Модель	PERCo-IPxx
Время ожидания подтверждения при верификации	5 сек.
=Запрещение ДЧ	
в РЕЖИМЕ РАБОТЫ "Контроль"	☐
в РЕЖИМЕ РАБОТЫ "Совещание"	☐
=Подтверждение от ДЧ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
=Защита от передачи идентификаторов (Antipass)	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
в РЕЖИМЕ РАБОТЫ "Охрана"	Нет
+Дополнительные входы, маскируемые при разблокировке ИУ	
+Дополнительные выходы, активизируемые при разблокировке ИУ	
+Дополнительные выходы, нормализируемые при разблокировке ИУ	
+Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов сотрудников	

- ✓ **Время ожидания подтверждения при верификации** - временной параметр, который устанавливает время, в течение которого контроллер будет ожидать подтверждения от верифицирующего устройства. В качестве верифицирующего устройства может быть использовано ДУ контроллера или программное обеспечение.
- ✓ **Запрещение ДУ** - параметр, который дает возможность запретить работу ДУ контроллера по разблокировке ИУ в направлении работы данного считывателя в выбранных режимах доступа. При установке данного параметра произвести разблокировку ИУ в этом направлении в выбранных режимах доступа будет невозможно.
- ✓ **Подтверждение от ДУ**. При помощи этого параметра можно указать как в выбранных режимах доступа при поднесении идентификатора к данному считывателю будет формироваться запрос на подтверждение от ДУ.

Подтверждение от ДУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Да
Да	
Верифицировать идентификаторы Сотрудников	
при проходе	☐
при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ	☐
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет

Можно гибко настроить условия верификации идентификаторов. Имеются следующие условия верификации:

- ✓ **при проходе** — верификация будет осуществляется при попытке прохода без каких-либо нарушений
- ✓ **при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ**— верификация будет осуществляется случае попытки повторного прохода без предварительного прохода в обратную сторону (параметр «Защита от передачи идентификаторов» должен быть установлен на значение «Мягкая или Жесткая»)
- ✓ **Защита от передачи идентификаторов** - параметр, который позволяет определить реакцию контроллера в случае попытки повторного прохода без предварительного прохода в обратную сторону. Для каждого из указанных режимов работы контроллера можно выбрать один из вариантов работы:

Нет
Нет
Мягкая
Жесткая

- ✓ **Нет**. Контроллер не осуществляет проверку факта повторного прохода по идентификатору, предъявленному к выбранному считывателю.
- ✓ **Мягкая**. Контроллер разрешит повторный проход по идентификатору, предъявленному к выбранному считывателю и при этом в журнале регистрации записывается событие о проходе с нарушением зональности.
- ✓ **Жесткая**. Контроллер запретит попытку повторного прохода при предъявлении идентификатора к выбранному считывателю и при этом в журнал регистрации записывается событие о запрете прохода по причине

Кроме перечисленных выше параметров можно указать дополнительные параметры, влияющие на действия контроллера при поднесении идентификатора:

Дополнительные входы, маскируемые при разблокировке ИУ	
☐ Критерий маскирования	На указанное время
☐ На указанное время	
Время	3 сек.
Дополнительный вход №1	☐
Дополнительный вход №2	☐
Дополнительные выходы, активизируемые при разблокировке ИУ	
Критерий активизации	На время срабатывания
Дополнительный выход №1	☐
Дополнительный выход №2	☐
Дополнительные выходы, нормализируемые при разблокировке ИУ	
☐ Критерий нормализации	На время срабатывания и после срабатывания
☐ На время срабатывания и после срабатывания	
Время	250 мс.
Дополнительный выход №1	☐
Дополнительный выход №2	☐
Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов сотрудников	
☐ Критерий активизации	На указанное время
☐ На указанное время	
Время	3 сек.
Дополнительный выход №1	☐
Дополнительный выход №2	☐

- ✓ **Дополнительные входы, маскируемые при разблокировке ИУ.** Этот параметр позволяет указать, какие именно дополнительные входы контроллера должны быть маскированы, т.е. не воспринимать управляющий сигнал от внешнего оборудования, при разблокировке ИУ. Для выбора отметьте флажки тех дополнительных входов, которые должны быть маскированы. Кроме этого, укажите временной критерий маскирования, который может быть одним из трех видов:

☐ Критерий маскирования	На указанное время
☐ На указанное время	На указанное время
Время	На время срабатывания
Дополнительный вход №2	На время срабатывания и после срабатывания

- ✓ **На указанное время** – выбранные дополнительные входы будут маскированы на указанное время.
- ✓ **На время срабатывания** – выбранные дополнительные входы будут маскированы на протяжении всего времени, когда ИУ будет разблокировано.
- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные входы будут маскированы на время, в течение которого ИУ будет разблокировано плюс указанное вами время.
- ✓ **Дополнительные выходы, активизируемые при разблокировке ИУ.** Этот параметр позволяет указать, какие именно дополнительные выходы контроллера

Критерий активизации	На указанное время
На указанное время	На указанное время
Время	На время срабатывания
Дополнительный выход №1	На время срабатывания и после срабатывания

- ✓ **На указанное время** – выбранные дополнительные выходы будут активизированы на указанное время.
 - ✓ **На время срабатывания** – выбранные дополнительные выходы будут активизированы на протяжении всего времени, когда ИУ будет разблокировано.
 - ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут активизированы на время, в течение которого ИУ будет разблокировано плюс указанное вами время.
- ✓ **Дополнительные выходы, нормализуемые при разблокировке ИУ.** Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализованы при разблокировке ИУ. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть нормализованы. Кроме этого, укажите временной критерий нормализации, который может быть одним из трех видов:

Критерий нормализации	На указанное время
На указанное время	На указанное время
Время	На время срабатывания
Дополнительный выход №1	На время срабатывания и после срабатывания

- ✓ **На указанное время** – выбранные дополнительные выходы будут нормализованы на указанное время.
 - ✓ **На время срабатывания** – выбранные дополнительные выходы будут нормализованы на протяжении всего времени, когда ИУ будет разблокировано.
 - ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут нормализованы на время, в течение которого ИУ будет разблокировано плюс указанное вами время.
- ✓ **Дополнительные выходы, активизируемые при предъявлении валидных пропусков.** Этот параметр позволяет указать те дополнительные выходы, которые будут активизированы на указанное время в случае предъявления не заблокированного и с не истекшим сроком действия идентификатора. Этот параметр может быть использован в случае, если к этим дополнительным выходам подключена дополнительная индикация, информирующая работников охраны о статусе предъявленной карты. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть активизированы. Кроме этого, укажите временной критерий активизации, который может быть одним из трех видов:

Критерий активизации	На указанное время
На указанное время	На указанное время
Время	На время срабатывания
Дополнительный выход №1	На время срабатывания и после срабатывания

- ✓ **На указанное время** – выбранные дополнительные выходы будут активизированы на указанное время начиная с момента предъявления идентификатора, независимо от того будет или нет разрешён проход.
- ✓ **На время срабатывания** – выбранные дополнительные выходы будут активизированы на указанное время начиная с момента разблокирования ИУ и до момента его заблокирования, либо, если проход не был совершён, по истечению времени анализа идентификатора.
- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут активизированы на указанное время начиная с момента разблокирования ИУ и до момента его заблокирования плюс указанное вами время, либо, если проход не был совершён, по истечению времени анализа идентификатора.

Генератор тревоги

В зависимости от структуры системы безопасности, ее задач, местоположения контроллера управления доступом, текущего режима доступа те или иные действия пользователей системы могут приводить к генерации тревоги.

Для выявления причин генерации тревоги и управления выделенным выходом тревоги (один из дополнительных выходов) определите следующие параметры:

Текущее наименование	Генератор тревоги №1
Первоначальное наименование	Генератор тревоги №1
Генерация тревоги при предъявлении идентификатора	
если ИДЕНТИФИКАТОР НЕ ЗАРЕГИСТРИРОВАН	Нет
если ИДЕНТИФИКАТОР ЗАПРЕЩЕН	Нет
если ИДЕНТИФИКАТОР ИЗ СТОП-ЛИСТА	Нет
если ИСТЕК СРОК ДЕЙСТВИЯ	Нет
если НАРУШЕНА ЗОНАЛЬНОСТЬ	Нет
если НАРУШЕН РЕЖИМ РАБОТЫ	Нет
Генерация тревоги при несанкционированной разблокировке ИУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
в РЕЖИМЕ РАБОТЫ "Закрето"	Нет
Генерация тревоги по недопустимо долгому открытию ИУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
Генерация тревоги по датчику вскрытия корпуса контроллера	Нет

- ✓ **Генерация тревоги при предъявлении идентификатора.** Этот параметр позволяет указать причины генерации тревожных события и перехода контроллера в состояние «Тревога» при предъявлении идентификатора с указанными параметрами доступа.

- ✓ **Генерация тревоги при несанкционированной разблокировке ИУ.** Этот параметр позволяет указать, будет ли контроллер автоматически генерировать тревожное событие и переходить в состояние «Тревога» в случае разблокировки ИУ при помощи ключа (то есть разблокировке ИУ без команды от контроллера) в выбранных режимах доступа.
- ✓ **Генерация тревоги по недопустимо долгому открытию ИУ.** Этот параметр позволяет указать, будет ли контроллер автоматически генерировать тревожное событие и переходить в состояние «Тревога» в случае, если после открытия ИУ оно не было приведено в исходное состояние в течение времени большего, чем указано в параметрах этого ИУ. Другими словами, должен ли контроллер перейти в состояние «Тревога», если после прохода через дверь она осталась открытой.
- ✓ **Генерация тревоги по датчику вскрытия корпуса контроллера**— параметр, который позволяет указать, будет ли контроллер автоматически генерировать тревожное событие, если его корпус был вскрыт.

Описание параметров функционирования контроллеров доступа (серия СТ/L04)

Подробная информация о параметрах функционирования контроллера СТ/L04 приведена в техническом описании системы безопасности.

Контроллер СТ/L04 — многофункциональный контроллер доступа. В зависимости от перемычек на печатной плате контроллер может быть сконфигурирован как:

- Контроллер для управления одной двухсторонней дверью
- Контроллер для управления одной двухсторонней дверью с подключением до 8 шт. контроллеров замка PERCo-CL201
- Контроллер для управления двумя односторонними дверьми с подключением до 8 шт. контроллеров замка PERCo-CL201
- Контроллер для управления турникетом с УИ
- Контроллер для управления турникетом с УИ с подключением до 8 шт. контроллеров замка PERCo-CL201

Ниже будут приведены общие рекомендации, проиллюстрированные примерами задания параметров ресурсов контроллеров.

Дополнительный вход

Дополнительные входы контроллеров могут быть использованы для наблюдения за состоянием внешнего оборудования, подключенного к ним, и для подключения кнопок сброса тревоги. Имеет два дополнительных входа.

В зависимости от того, какое внешнее оборудование подключено к дополнительному входу, существуют следующие варианты описания параметров его работы:

Текущее наименование	Дополнительный вход №1
Адрес	1
Первоначальное наименование	Дополнительный вход №1
☐ Тип	Обычный
☐ Обычный	
Нормальное состояние контакта	Разомкнут
☐ Дополнительные входы, маскируемые при активизации	
☐ Критерий маскирования	На указанное время
☐ На указанное время	
Время	3 сек.
Дополнительный вход №2	☒
☐ Дополнительные выходы, активизируемые при активизации	
☐ Критерий активизации	На указанное время
☒ На указанное время	
Дополнительный выход №1	☒
☐ Дополнительные выходы, нормализируемые при активизации	
☒ Критерий нормализации	На указанное время
Дополнительный выход №1	☐

- ✓ При условии, что к данному дополнительному входу не подключено никакое внешнее оборудование, менять параметры работы дополнительного входа не нужно.
- ✓ **Нормальное состояние контакта** (нормально замкнут / нормально разомкнут). Этот параметр зависит от типа подключенного оборудования и указывает контроллеру на то, какое значение уровня сигнала на данном дополнительном входе он должен воспринимать как нормальное.
- ✓ Тип дополнительного входа – **обычный**. Означает что к данному дополнительному входу подключено внешнее оборудование, состояние которого должно контролироваться контроллером. При выборе этого типа можно так же указать алгоритм действий контроллера при получении управляющего воздействия от подключенного оборудования, а именно:

- **Дополнительные входы, маскируемые при активизации.** Этот параметр позволяет указать, какие именно дополнительные входы контроллера должны быть маскированы, т.е. не воспринимать управляющий сигнал от внешнего оборудования, при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте флажки тех дополнительных входов, которые должны быть маскированы. Кроме этого, укажите временной критерий маскирования, который может быть одним из трех видов:

☐ Критерий маскирования	На указанное время
☐ На указанное время	На указанное время
Время	На время срабатывания
Дополнительный вход №2	На время срабатывания и после срабатывания

- ✓ **На указанное время** – выбранные дополнительные входы будут маскированы на указанное время.

- ✓ **На время срабатывания** – выбранные дополнительные входы будут маскированы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.
- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные входы будут маскированы на время, в течение которого на данном дополнительном входе будет присутствовать управляющий сигнал плюс указанное вами время.
- **Дополнительные выходы, активизируемые при активизации.** Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть активизированы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть активизированы. Кроме этого, укажите временной критерий активизации, который может быть одним из трех видов:

☐ Критерий активизации	На указанное время
☐ На указанное время	На указанное время
☐ Время	На время срабатывания
☐ Дополнительный выход №1	На время срабатывания и после срабатывания

- ✓ **На указанное время** – выбранные дополнительные выходы будут активизированы на указанное время.
- ✓ **На время срабатывания** – выбранные дополнительные выходы будут активизированы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.
- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут активизированы на время, в течение которого на данном дополнительном входе будет присутствовать управляющий сигнал плюс указанное вами время.
- **Дополнительные выходы, нормализуемые при активизации.** Этот параметр позволяет указать, какие именно дополнительные выходы контроллера должны быть нормализованы при получении управляющего сигнала от подключенного к данному дополнительному входу оборудования. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть нормализованы. Кроме этого, укажите временной критерий нормализации, который может быть одним из трех видов:

☐ Критерий нормализации	На указанное время
☐ На указанное время	На указанное время
☐ Время	На время срабатывания
☐ Дополнительный выход №1	На время срабатывания и после срабатывания

- ✓ **На указанное время** – выбранные дополнительные выходы будут нормализованы на указанное время.
- ✓ **На время срабатывания** – выбранные дополнительные выходы будут нормализованы на протяжении всего времени, когда на данном дополнительном входе будет присутствовать управляющий сигнал.
- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут нормализованы на время, в течение которого

на данном дополнительном входе будет присутствовать управляющий сигнал плюс указанное вами время.

Тип входа – **Специальный**. Предназначен для автономного сброса тревоги в состоянии «Тревога как СКУД» либо выключения sireны в состоянии «Тревога как ОПС».

Текущее наименование	Дополнительный вход №2
Адрес	2
Первоначальное наименование	Дополнительный вход №2
Тип	Специальный
Специальный	
Нормальное состояние контакта	Разомкнут
Сброс тревоги (Генератор тревоги)	☐
Сброс sireны (Выход "С" ОПС)	☐

Если данный дополнительный вход используется как вход автономного сброса тревоги, укажите, какой тип тревоги, которая будет сбрасываться при поступлении управляющего сигнала на этот дополнительный вход.

Возможны два варианта:

- ✓ **Сброс тревоги (Генератор тревоги).** В этом случае при возникновении тревоги из-за ситуации, описанной в генераторе тревоги, получение управляющего сигнала на данном дополнительном входе приведет к ее сбросу.
- ✓ **Сброс sireны (Выход «С» ОПС).** Аналогично предыдущему, но будет выключена sireна, подключенная к выходу «С» ОПС.

Дополнительный выход

Дополнительные выходы могут быть использованы для управления любым дополнительным оборудованием в рамках системы безопасности. Технические параметры дополнительных выходов для каждого типа контроллера приведены в техническом описании системы безопасности. Имеется от двух до четырех дополнительных выходов в зависимости от типа контроллера.

В зависимости от алгоритма работы внешних устройств, подключенных к дополнительному выходу существуют следующие варианты описания параметров работы выхода:

- ✓ При условии, что к данному дополнительному выходу не подключено никакое дополнительное оборудование, менять параметры работы выхода не нужно.
- ✓ Тип дополнительного выхода – **Обычный**

Текущее наименование	Дополнительный выход №2
Адрес	2
Первоначальное наименование	Дополнительный выход №2
Тип	Обычный
Обычный	
Нормальное состояние	Не запитан

Этот параметр указывает, что к данному дополнительному выходу подключено дополнительное оборудование, логика управления которым описывается через описание других устройств системы (за исключением генератора тревоги). Задайте нормальное состояние контактов для данного дополнительного выхода. Существуют два варианта – запитан/незапитан. Этот параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий.

- ✓ Тип дополнительного выхода – **генератора тревоги**.

Текущее наименование	Дополнительный выход №3
Адрес	3
Первоначальное наименование	Дополнительный выход №3
Тип	Генератора тревоги
Генератора тревоги	
Нормальное состояние	Не запитан
Время активизации	1 сек.

В этом случае решение об активизации дополнительного выхода принимается исключительно панелью в соответствии с параметрами, указанными в ее генераторе тревоги. Этот дополнительный выход будет использоваться для индикации перехода панели в состояние «Тревога». Так же задайте нормальное состояние контактов для данного дополнительного выхода. Существуют два варианта – запитан/не запитан. Этот параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий. Кроме этого, укажите время активизации дополнительного выхода, время, в течение которого при наличии активизирующего управляющего воздействия выход меняет своё состояние из нормализованного на противоположное. Как правило, в этом случае к такому дополнительному выходу подключают тревожный оповещатель (сирена, проблесковая лампа).

- ✓ Тип дополнительного выхода – **ОПС**.

Текущее наименование	Дополнительный выход №1
Адрес	1
Первоначальное наименование	Дополнительный выход №1
Тип	ОПС
ОПС	
Нормальное состояние	Не запитан
Задержка перед запуском	0 мс.
Время активизации	1 сек.
Программа управления	Не управлять
Зоны, активизирующие выход	
Зона №11	☐
Зона №12	☐
Зона №1	☐
Зона №2	☐
Зона №3	☐

В этом случае дополнительный выход предназначен для управления световым оповещением (СО), звуковым оповещением (ЗО), а так же для передачи тревожных извещений на пульт центрального наблюдения (ПЦН) при изменении режимов и состояний охранной зоны (ОЗ).

Задайте нормальное состояние контактов для данного дополнительного выхода. Существуют два варианта – запитан/не запитан. Этот параметр определяет состояние контактов реле при отсутствии на нем активизирующих воздействий.

Программа управления задает логику работы панели по управлению этим дополнительным выходом. Инициатором активизации выхода являются изменения режимов и состояний зон, отмеченных под параметром «Зоны, активизирующие выход». После возникновения события, инициирующего активизацию выхода (в соответствии с заданной программой), начинается отсчёт задержки, указанной в параметре «Задержка перед запуском» (если задержка ненулевая), по окончании которой выход активизируется. В зависимости от программы управления выход может быть запитан (не запитан) постоянно (пока ресурс панели находится в текущем режиме), либо изменять своё физическое состояние (мигать) из нормализованного на противоположное. Нормализация выхода происходит либо по истечению времени, указанному в параметре «Время активизации» (если оно не бесконечное), либо по сбросу панели, либо после выключения ее питания. После включения питания все выходы нормализуются.

Вид программы выбирается из выпадающего списка. Возможны следующие варианты программ управления дополнительным выходом:

- ✓ **Включить при тревоге.** В случае перехода одной из зон в режим «ТРЕВОГА» произойдет замыкание контакта дополнительного выхода.
- ✓ **Мигать при тревоге.** В случае перехода одной из зон в режим «ТРЕВОГА» произойдет попеременное размыкание - замыкание контактов дополнительного выхода.
- ✓ **Лампа 1** – программа управления, указывающая на то, что к дополнительному выходу подключен световой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы все зоны изменили свой режим.

- ✓ **Лампа 2** – программа управления, указывающая на то, что к дополнительному выходу подключен световой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы хотя бы одна из зон изменила свой режим.
- ✓ **ПЦН 1** – программа управления, указывающая на то, что дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН). Для активизации программы требуется, чтобы все зоны изменили свой режим.
- ✓ **ПЦН 2** – программа управления, указывающая на то, что дополнительный выход используется для передачи тревожного извещения на пост центрального наблюдения (ПЦН). Для активизации программы требуется, чтобы все зоны изменили свой режим.
- ✓ **Сирена** – программа управления, указывающая на то, что к дополнительному выходу подключен звуковой оповещатель тревожной ситуации. Для активизации программы требуется, чтобы хотя бы одна из зон изменила свой режим.
- ✓ **Включить перед взятием** – Перед переходом одной из зон в режим «ВЗЯТИЕ» произойдет замыкание контакта дополнительного выхода.
- ✓ **Включить при взятии** — При переходе одной из зон в режим «ВЗЯТИЕ» произойдет замыкание контакта дополнительного выхода.
- ✓ **Включить при снятии** – Перед переходом одной из зон в режим «СНЯТА» произойдет замыкание контакта дополнительного выхода.
- ✓ **Включить при автоперевзятии** – При переходе одной из охранных зон в режим «АВТОПЕРЕВЗЯТИЕ» произойдет замыкание контакта дополнительного выхода.

Шлейф сигнализации

Контроллеры имеют возможность подключения стандартных шлейфов охранной сигнализации. Использование охранных шлейфов позволяет системе безопасности контролировать не только вход в помещение, но и внутренний объем помещения, открывание окон и так далее за счет подключения дополнительных охранных датчиков. Имеется до двух охранных шлейфов сигнализации в зависимости от типа контроллера.

В зависимости от алгоритма работы внешних датчиков и извещателей, подключенных к шлейфу сигнализации существуют следующие варианты описания параметров работы шлейфа:

- ✓ Тип шлейфа сигнализации — **Охранный**

Текущее наименование	Шлейф сигнализации №1
Адрес	1
Первоначальное наименование	Шлейф сигнализации №1
Тип	Охранный ▼
Охранный	
Контроль вскрытия корпуса извещателей	☐
Поддержка перезапроса	☐
Длительность нарушения	70 мс.
Задержка взятия на охрану	0 мс.
Задержка восстановления нарушенного шлейфа в снятом состоянии	0 мс.

- ✓ **Контроль вскрытия корпуса извещателей** — параметр, указывающий шлейфу контролировать вскрытие корпуса извещателей.

- ✓ **Поддержка перезапроса** - параметр, определяющий, надо или нет после срабатывания извещателей снимать питание с шлейфа и перепроверять его состояние.
- ✓ **Длительность нарушения** - параметр, определяющий для шлейфа время интегрирования
- ✓ **Задержка взятия на охрану** — параметр, определяющий для шлейфа время, через которое панель предпринимает попытку взять шлейф на охрану после поступления соответствующей команды.
- ✓ **Задержка восстановления нарушенного шлейфа в снятом состоянии** — если данный параметр установлена в 0, то шлейф в состоянии «СНЯТ» не контролируется. В противном случае продолжается отслеживание шлейфа в режиме «Снят». Если при этом шлейф перейдет в состояние «НАРУШЕНИЕ», то в журнал регистраций записывается событие «Неисправность снятого ОШС», состояние выходов и встроенная звуковая индикация панели не изменяются. Если после этого нормальное состояние шлейфа восстановится и продержится время, указанное в этом параметре, то шлейф выйдет из состояния «НАРУШЕНИЕ» и при этом в журнал регистраций будет записано сообщение «Нормализация снятого ОШС». Состояние выходов и встроенная звуковая индикация панели не изменяются.

Зоны

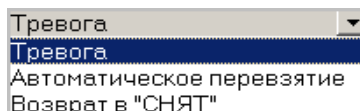
Зона – логическая структура, которая позволяет создать комбинации ресурсов контроллера, которые будут ставиться на охрану в зависимости от прав пользователя системы. Имеется до двенадцати зон в зависимости от типа контроллера.

Имеются следующие параметры:

Текущее наименование	Зона №1
Адрес	1
Первоначальное наименование	Зона №1
Включить ИУ в зону	☒
Повторное включение сирены	☐
Режим работы при невзятии	Тревога
☐ Не активизировать при тревоге по Охранным шлейфам сигнализации	
Выходы, работающие по программе "Сирена" или "Лампа"	☐
☐ Шлейфы, активизирующие зону	
Шлейф сигнализации №1	☐
Шлейф сигнализации №2	☐

- ✓ **Включить ИУ в зону** – параметр, указывающий на то, входит ли исполнительное устройство в эту зону. То есть, если исполнительное устройство добавлено в зону, при постановке на охрану контроллер будет контролировать его состояние. В противном случае открытие двери не будет приводить к возникновению тревоги после постановки зоны на охрану. Это может быть использовано в том случае, когда ресурсы контроллера используются не только для контроля помещения, доступ в которое он контролирует.
- ✓ **Повторное включение сирены** - параметр, позволяющий реализовать тактику активизации дополнительного выхода, управляемого по программе "Сирена" при каждом нарушении зоны, даже если она уже находится в режиме "Тревога".

- ✓ **Режим работы при невзятии** — параметр указывает действие, которое будет происходить при невозможности взятия данной зоны на охрану. Имеются следующие значения:



- **Тревога** — зона будет переведена в режим «ТРЕВОГА».
 - **Автоматическое перевзятие** — зона будет переведена в режим «Взятие», а затем, будет производится повторная попытка взятия до тех пор, пока взятие не произойдет.
 - **Возврат в режим снят** — зона перейдет в режим «СНЯТА».
- ✓ **Не активизировать при тревоге по охранным шлейфам сигнализации дополнительные выходы, работающие по программе «Сирена» или «Лампа»** - параметр указывает, нужно ли в случае тревоги в данной зоне запрещать активизацию дополнительных выходов, работающие по программе управления «Сирена» или «Лампа».
 - ✓ **Шлейфы, активизирующие зону.** Параметр позволяет указать, шлейфы сигнализации, которые будут контролироваться контроллером при постановке зоны на охрану.

Исполнительное устройство

Данный контроллер может управлять от одного до десяти исполнительными устройствами. Количество и тип исполнительных устройств определяется типом контроллера. Так как контроллер не может автоматически определять параметры функционирования исполнительных устройств, следует задать эти параметры. Для этого выберите исполнительное устройство у контроллера. В правой части в панели параметров будут отображены все возможные параметры функционирования.

Для контроллера управления замком или турникетом:

Текущее наименование	Турникет
Первоначальное наименование	Турникет
Прямое направление прохода	☒
Нормальное (т.е заблокированное) состояние контакта (вход ИУ)	Нормально замкнут
Нормальное состояние "Закрыто" выхода ИУ	Не запитан
Нормализация выхода ИУ	После "Открытия"
Предельное время разблокировки	8 сек.
Время удержания в разблокируемом состоянии (время анализа идентификатора)	4 сек.
Регистрация прохода по предъявлению идентификатора	☐
Внутренняя защита от передачи идентификаторов (Local Antipass)	☐

Большинство параметров идентичны для всех типов контроллеров. Отличительные особенности будут описаны ниже после описания основных параметров. Ниже приведено описание параметров исполнительного устройства:

- ✓ **Прямое направление прохода.** Данный параметр определяет, в какую сторону будет разблокирован ИУ при предъявлении карты к первому считывателю контроллера.
- ✓ **Нормальное (т.е. заблокированное) состояние контакта (вход ИУ).** Параметр описывает состояние датчика двери/турникета. В зависимости от его конструкции он может быть при закрытом ИУ замкнут (как правило, герконы двери) или разомкнут.
- ✓ **Нормальное состояние «Закрыто» выхода ИУ.** Параметр описывает должен ли контроллер подавать напряжение на ИУ в состоянии «Закрыто». Так, например, для электромагнитных замков в состоянии «Закрыто» необходимо подавать напряжение на ИУ, для электромеханических такой необходимости нет.
- ✓ **Нормализация выхода ИУ.** Параметр описывает, в какой момент времени контроллер должен начать свои действия по блокировке ИУ (сразу после открытия ИУ или после его закрытия). Факт открытия/закрытия ИУ контроллер определяет по датчику, установленному на вход ИУ.
- ✓ **Режим работы выхода управления ИУ.** описывает логику управления подключенным исполнительным устройством. Его значение определяется исходя из параметров работы подключенного устройства.
- ✓ **Предельное время разблокировки** описывает время, по истечении которого контроллер перейдет в состояние тревога по причине того, что исполнительное устройство не заблокировано.
- ✓ **Время удержание в разблокированном состоянии** (время анализа идентификатора) описывает время, по истечении которого контроллер управления доступом переведет исполнительное устройство в состояние «Закрыто». Снимет управляющий сигнал с линии управления исполнительным устройством.
- ✓ **Регистрация прохода по предъявлению идентификатора** указывает на то, что контроллер будет считать проход совершившимся сразу после поднесения идентификатора доступа к его считывателю, игнорируя информацию о сигнале, получаемом с датчика ИУ.
- ✓ **Внутренняя защита от передачи идентификаторов** задает режим работы контроллера по контролю за повторными входами. При отмеченной опции, контроллер будет блокировать попытки повторного входа/выхода.

Считыватель

В зависимости от типа используемого контроллера количество считывателей может быть от двух до десяти.

Задание параметров функционирования считывателей фактически определяет порядок и условия работы контроллера при предъявлении идентификатора доступа. Часть параметров считывателя определяют параметры разрешения прохода в направлении, контролируемом данным считывателем.

Текущее наименование	Главный вход
Первоначальное наименование	Считыватель №1
Модель	PERCo-IPxx
☐ <u>Запрещение ДУ</u>	
в РЕЖИМЕ РАБОТЫ "Контроль"	☐
в РЕЖИМЕ РАБОТЫ "Совещание"	☐
☐ <u>Подтверждение от ДУ</u>	
☐ в РЕЖИМЕ РАБОТЫ "Контроль"	Да
☐ в РЕЖИМЕ РАБОТЫ "Совещание"	Да
Время ожидания подтверждения при верификации	5 сек.
☐ <u>Защита от передачи идентификаторов (Antipass)</u>	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
в РЕЖИМЕ РАБОТЫ "Охрана"	Нет
☐ <u>Дополнительные входы, маскируемые при разблокировке ИУ</u>	
☐ <u>Дополнительные выходы, активизируемые при разблокировке ИУ</u>	
☐ <u>Дополнительные выходы, нормализируемые при разблокировке ИУ</u>	
☐ <u>Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов сотрудников</u>	

- ✓ **Запрещение ДУ** - параметр, который дает возможность запретить работу ДУ контроллера по разблокировке ИУ в направлении работы данного считывателя в выбранных режимах доступа. При установке данного параметра произвести разблокировку ИУ в этом направлении в выбранных режимах доступа будет невозможно.
- ✓ **Время ожидания подтверждения при верификации** - временной параметр, который устанавливает время, в течение которого контроллер будет ожидать подтверждения от верифицирующего устройства. В качестве верифицирующего устройства используется ДУ контроллера.
- ✓ **Подтверждение от ДУ**. При помощи этого параметра можно указать как в выбранных режимах доступа при поднесении идентификатора к данному считывателю будет формироваться запрос на подтверждение от ДУ.

☐ <u>Подтверждение от ДУ</u>	
☐ в РЕЖИМЕ РАБОТЫ "Контроль"	Да
☐ <u>Да</u>	
☐ <u>Верифицировать идентификаторы Сотрудников</u>	
при проходе	☐
при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ	☐
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет

Можно гибко настроить условия верификации идентификаторов сотрудников/учеников .
Имеются следующие условия верификации :

- ✓ **при проходе** — верификация будет осуществляется при попытке прохода без каких-либо нарушений
- ✓ **при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ**— верификация будет осуществляется случае попытки повторного прохода без предварительного прохода в обратную сторону (параметр «**Защита от передачи идентификаторов**» должен быть установлен на значение «Мягкая или Жесткая»)

- ✓ **Защита от передачи идентификаторов** - параметр, который позволяет определить реакцию контроллера в случае попытки повторного прохода без предварительного прохода в обратную сторону. Для каждого из указанных режимов работы контроллера можно выбрать один из вариантов работы:

- ✓ **Нет.** Контроллер не осуществляет проверку факта повторного прохода по идентификатору, предъявленному к выбранному считывателю.
- ✓ **Мягкая.** Контроллер разрешит повторный проход по идентификатору, предъявленному к выбранному считывателю и при этом в журнале регистрации записывается событие о проходе с нарушением зональности.
- ✓ **Жесткая.** Контроллер запретит попытку повторного прохода при предъявлении идентификатора к выбранному считывателю и при этом в журнал регистрации записывается событие о запрете прохода по причине нарушения зональности, а в журнале мониторинга — событие о предъявлении такого идентификатора.

Кроме перечисленных выше параметров можно указать дополнительные параметры, влияющие на действия контроллера при поднесении идентификатора:

☐ <u>Дополнительные входы, маскируемые при разблокировке ИУ</u>	
☐ Критерий маскирования	На указанное время
☐ <u>На указанное время</u>	
Время	4 сек.
Дополнительный вход №1	☐
Дополнительный вход №2	☐
☐ <u>Дополнительные выходы, активизируемые при разблокировке ИУ</u>	
Критерий активизации	На время срабатывания
Дополнительный выход №1	☐
☐ <u>Дополнительные выходы, нормализируемые при разблокировке ИУ</u>	
☐ Критерий нормализации	На время срабатывания и после срабатывания
☐ <u>На время срабатывания и после срабатывания</u>	
Время	250 мс.
Дополнительный выход №1	☐
☐ <u>Дополнительные выходы, активизируемые при предъявлении валидных идентификаторов сотрудников</u>	
☐ Критерий активизации	На указанное время
☐ <u>На указанное время</u>	
Время	4 сек.
Дополнительный выход №1	☐

- ✓ **Дополнительные входы, маскируемые при разблокировке ИУ.** Этот параметр позволяет указать, какие именно дополнительные входы контроллера должны быть маскированы, т.е. не воспринимать управляющий сигнал от внешнего оборудования, при разблокировке ИУ. Для выбора отметьте флажки тех дополнительных входов, которые должны быть маскированы. Кроме этого, укажите временной критерий маскирования, который может быть одним из трех видов:

☐ Критерий маскирования	На указанное время
☐ На указанное время	На указанное время
Время	На время срабатывания
Дополнительный вход №2	На время срабатывания и после срабатывания

- ✓ **На указанное время** – выбранные дополнительные входы будут маскированы на указанное время.
 - ✓ **На время срабатывания** – выбранные дополнительные входы будут маскированы на протяжении всего времени, когда ИУ будет разблокировано.
 - ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные входы будут маскированы на время, в течение которого ИУ будет разблокировано плюс указанное вами время.
- ✓ **Дополнительные выходы, активизируемые при предъявлении валидных пропусков сотрудников.** Этот параметр позволяет указать те дополнительные выходы, которые будут активизированы на указанное время в случае предъявления не заблокированного и с не истёкшим сроком действия идентификатора сотрудника/ученика. Этот параметр может быть использован в случае, если к этим дополнительным выходам подключена дополнительная индикация, информирующая работников охраны о статусе предъявленной карты. Для выбора отметьте флажки тех дополнительных выходов, которые должны быть активизированы. Кроме этого, укажите временной критерий активизации, который может быть одним из трех видов:

☐ Критерий активизации	На указанное время
☐ На указанное время	На указанное время
Время	На время срабатывания
Дополнительный выход №1	На время срабатывания и после срабатывания

- ✓ **На указанное время** – выбранные дополнительные выходы будут активизированы на указанное время начиная с момента предъявления идентификатора, независимо от того будет или нет разрешён проход.
- ✓ **На время срабатывания** – выбранные дополнительные выходы будут активизированы на указанное время начиная с момента разблокирования ИУ и до момента его заблокирования, либо, если проход не был совершён, по истечению времени анализа идентификатора.
- ✓ **На время срабатывания и после срабатывания** – выбор этого параметра является комбинацией двух предыдущих. Выбранные дополнительные выходы будут активизированы на указанное время начиная с момента разблокирования ИУ и до момента его заблокирования плюс указанное вами время, либо, если проход не был совершён, по истечению времени анализа идентификатора.

Генератор тревоги

В зависимости от структуры системы безопасности, ее задач, местоположения контроллера управления доступом, текущего режима доступа те или иные действия пользователей системы могут приводить к генерации тревоги.

Для выявления причин генерации тревоги и управления выделенным выходом тревоги (один из дополнительных выходов) определите следующие параметры:

Текущее наименование	Генератор тревоги №1
Первоначальное наименование	Генератор тревоги №1
Генерация тревоги при предъявлении идентификатора	
если ИДЕНТИФИКАТОР НЕ ЗАРЕГИСТРИРОВАН	Нет
если ИДЕНТИФИКАТОР ЗАПРЕЩЕН	Нет
если ИДЕНТИФИКАТОР ИЗ СТОП-ЛИСТА	Нет
если ИСТЕК СРОК ДЕЙСТВИЯ	Нет
если НАРУШЕНА ЗОНАЛЬНОСТЬ	Нет
если НАРУШЕН РЕЖИМ РАБОТЫ	Нет
Генерация тревоги при несанкционированной разблокировке ИУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
в РЕЖИМЕ РАБОТЫ "Закрето"	Нет
Генерация тревоги по недопустимо долгому открытию ИУ	
в РЕЖИМЕ РАБОТЫ "Контроль"	Нет
в РЕЖИМЕ РАБОТЫ "Совещание"	Нет
Генерация тревоги по датчику вскрытия корпуса контроллера	Нет

- ✓ **Генерация тревоги при предъявлении идентификатора.** Этот параметр позволяет указать причины генерации тревожных события и перехода контроллера в состояние «Тревога» при предъявлении идентификатора с указанными параметрами доступа.
- ✓ **Генерация тревоги при несанкционированной разблокировке ИУ.** Этот параметр позволяет указать, будет ли контроллер автоматически генерировать тревожное событие и переходить в состояние «Тревога» в случае разблокировки ИУ при помощи ключа (то есть разблокировке ИУ без команды от контроллера) в выбранных режимах доступа.
- ✓ **Генерация тревоги по недопустимо долгому открытию ИУ.** Этот параметр позволяет указать, будет ли контроллер автоматически генерировать тревожное событие и переходить в состояние «Тревога» в случае, если после открытия ИУ оно не было приведено в исходное состояние в течение времени большего, чем указано в параметрах этого ИУ. Другими словами, должен ли контроллер перейти в состояние «Тревога», если после прохода через дверь она осталось открытой.
- ✓ **Генерация тревоги по датчику вскрытия корпуса контроллера**– параметр, который позволяет указать, будет ли контроллер автоматически генерировать тревожное событие, если его корпус был вскрыт.

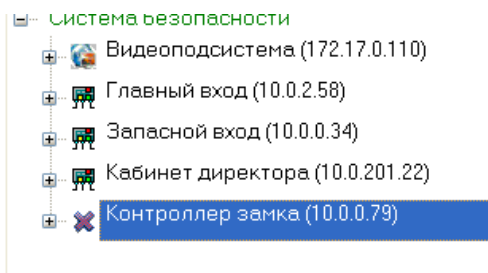
Исключение из конфигурации

В зависимости от построения системы безопасности и в процессе работы может возникнуть ситуация, при которой необходимо исключить то или иное устройство из конфигурации. Например, устройство было демонтировано, вышло из строя и заменено другим или устройство было найдено в результате проведения конфигурации, но работает

под управлением другого программного обеспечения. В этом случае необходимо исключить его из конфигурации.

Для исключения из конфигурации (но не удаления из списка устройств):

1. Выделите устройство, которое подлежит исключению из конфигурации.
2. Щелкните на кнопке **Исключить из конфигурации** — . Слева от устройства появится значок , который указывает на то, что устройство находится вне конфигурации:



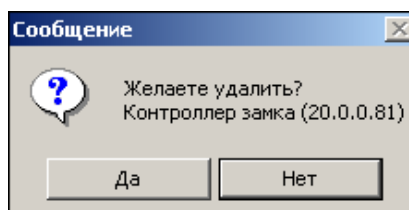
Удаление устройства

Так как исключение из конфигурации не приводит к удалению устройства из списка устройств, что может привести к неудобству работы, его можно удалить из конфигурации. При удалении информация об этом устройстве останется в данных программы для последующего восстановления см. п. «[Удаленные устройства](#)».

Удаляется устройство, если оно исключено из конфигурации (см. п. «[Исключение из конфигурации](#)» выше).

Для удаления устройства:

1. Выделите устройство, которое подлежит удалению.
2. Щелкните на кнопке **Удалить** — . Откроется окно подтверждения:



3. После подтверждения устройство перестанет отображаться в списке устройств.



ПРИМЕЧАНИЕ

Устройство, прикрепленное к какому-нибудь помещению, не удалится, а скроется. Кнопка **Отображать скрытые устройства** —  позволяет увидеть в списке скрытые устройства.

Удаленные устройства

Программное обеспечение системы безопасности позволяет восстановить ранее удаленные из конфигурации устройства. Это может быть актуально при изменении структуры системы безопасности, при проведении пусконаладочных работ. Восстановить можно только скрытое устройство. Чтобы восстановить удаленное, нужно либо заново провести конфигурацию, либо

воспользоваться кнопкой **Добавить новое устройство** — .

Для восстановления удаленного устройства:

1. Щелкните на кнопке **Отображать скрытые устройства/Восстановить удаленное устройство** — . Эта кнопка только отображает скрытые устройства, выделенные шрифтом красного цвета. Восстановить скрытое устройство можно, если щелкнуть еще раз на кнопке **Удалить/Восстановить** — .
2. Значок  слева от устройства указывает на то, что устройство находится вне конфигурации.
3. Щелкните на кнопке **Включить в конфигурацию** — . Слева от устройства появится значок , который указывает на то, что устройство отключено, но включено в конфигурацию.
4. Передайте измененные параметры в аппаратуру с помощью кнопки .

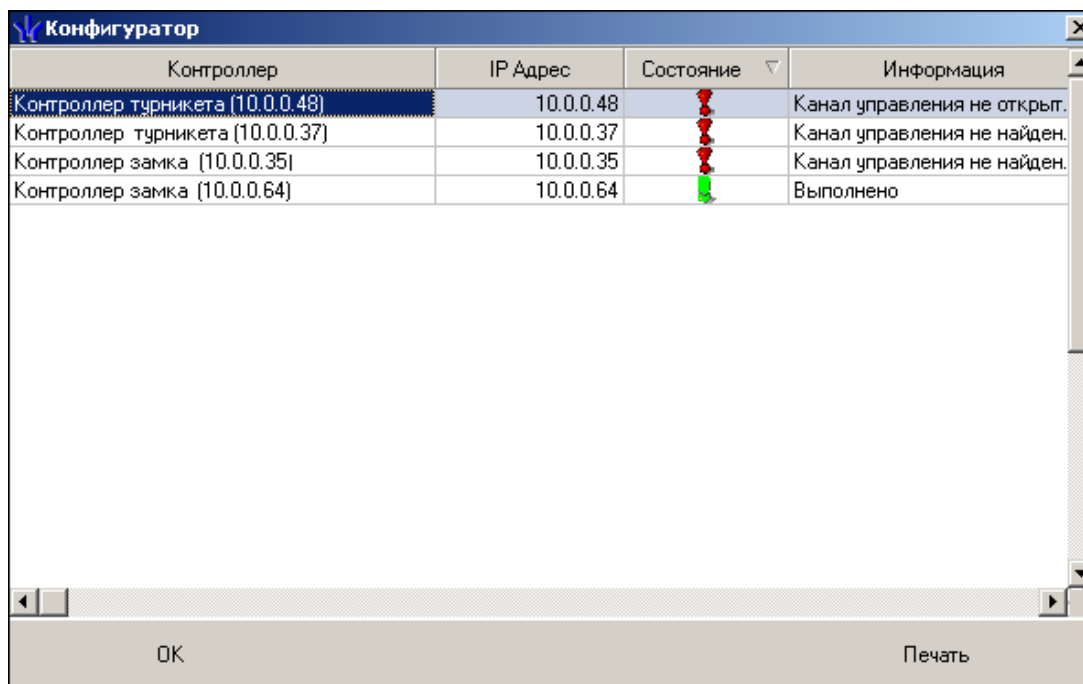
Передача параметров устройства

Любое устройство, входящее в состав системы безопасности, имеет характерный для него набор параметров функционирования. Эти параметры могут быть изменены пользователем в соответствии с необходимым алгоритмом работы. Порядок внесения изменений в параметры работы устройств описан ниже. Более подробную информацию о параметрах каждого устройства, их назначении вы можете получить в техническом описании на интересующее вас устройство.

Для передачи параметров устройства:

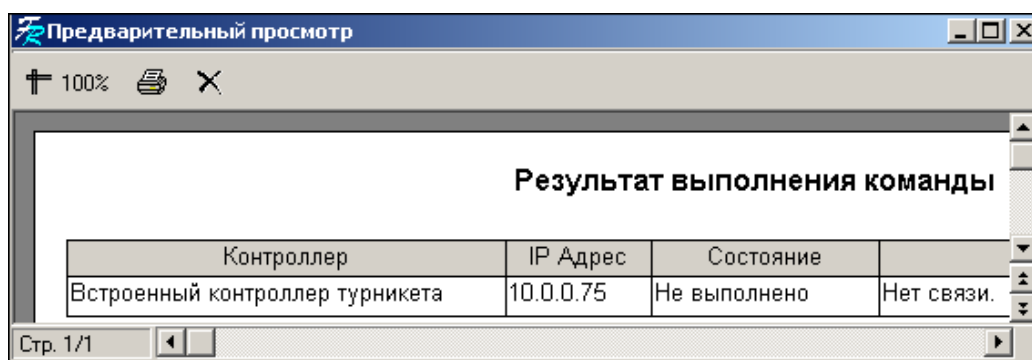
1. Выделите устройство, чьи параметры подлежат передаче в систему.
2. Щелкните на кнопке **Передать параметры** — . Курсор мыши примет форму , и в строке состояния будет отображаться ход процесса передачи данных в устройство.

В случае если программное обеспечение не сможет передать данные в устройство будет выведено информационное окно, с указанием причин невозможности передачи данных:



3. Для закрытия окна щелкните на кнопке «ОК».

Кнопка **Печать** выведет на экран окно предварительного просмотра результатов выполнения команды:



Масштаб — 100% — для настройки изображения документа на экране.

Печать отчёта — — для вывода документа на печать.

Выход — для выхода из режима предварительного просмотра в окно раздела Конфигуратор.

Передача измененных параметров устройства

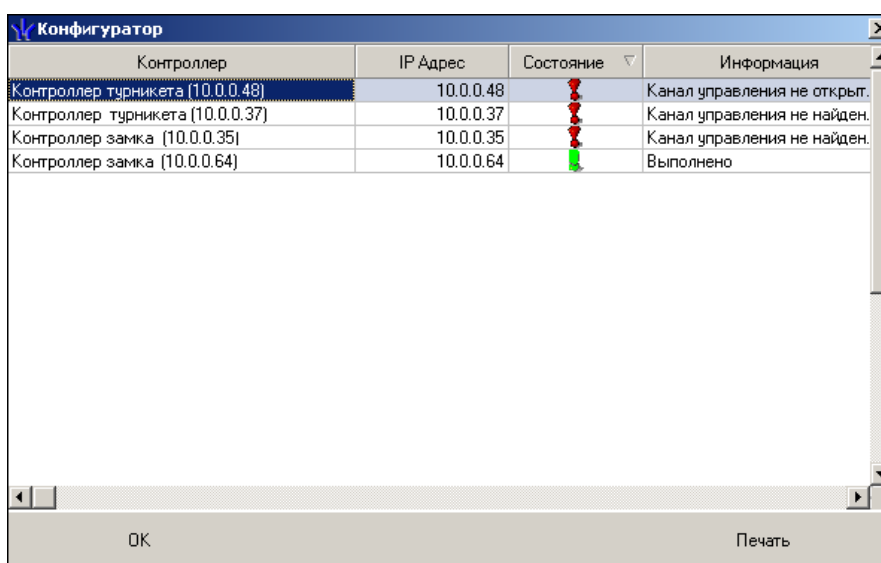
Как правило, в процессе работы системы может возникнуть необходимость внести те или иные изменения в параметры работы устройств. В этом случае предоставляется возможность передать в устройство, **только измененные** параметры. Этот способ передачи данных уменьшает время передачи и нагрузку на устройство.

Для передачи измененных параметров устройства:

1. Выделите устройство, чьи параметры были изменены.
2. Щелкните на кнопке **Передать измененные параметры** — . Курсор мыши

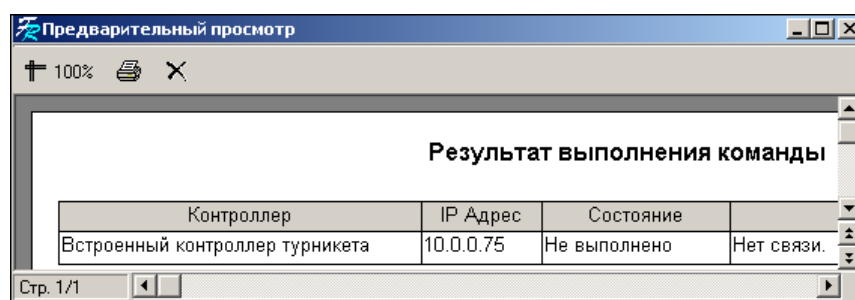
примет форму — , и в строке состояния будет отображаться ход процесса передачи данных в устройство.

В случае если программное обеспечение не сможет передать данные в устройство будет выведено информационное окно, с указанием причин невозможности передачи данных:



3. Для закрытия окна щелкните на кнопке «ОК».

Кнопка **Печать** выведет на экран окно предварительного просмотра результатов выполнения команды:



Масштаб —  100% — для настройки изображения документа на экране.

Печать отчёта —  — для вывода документа на печать.

Выход — для выхода из режима предварительного просмотра в окно раздела Конфигуратор.



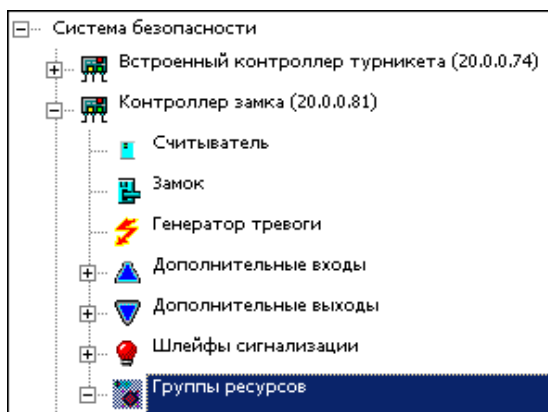
ПРИМЕЧАНИЕ

Передача измененных параметров занимает меньше времени, чем передача всех параметров системы.

Добавление группы ресурсов

Группа ресурсов – логическая структура, которая позволяет создать комбинации ресурсов контроллера, которые будут ставиться на охрану в зависимости от прав пользователя системы. Для добавления группы ресурсов:

- Выделите группу ресурсов:



- Щелкните на кнопке **Добавить группу ресурсов** — . В списке отобразится новая группа ресурсов.



ПРИМЕЧАНИЕ

Максимальное количество групп ресурсов 7.

Изменение пароля

Пароль устанавливают после завершения монтажа и пуска системы, тем самым, защищая контроллеры от несанкционированного подключения, как любое сетевое устройство.

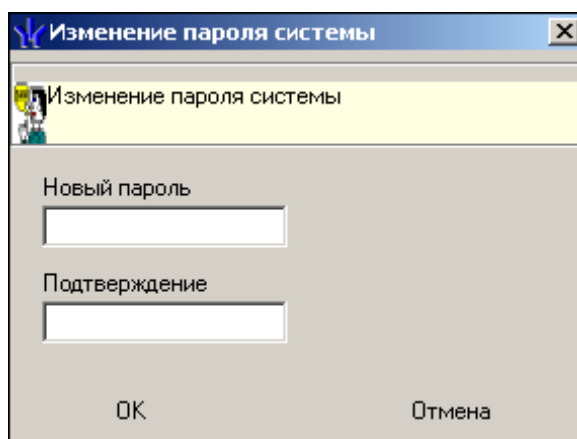
Для защиты контроллеров, входящих в состав системы безопасности, от несанкционированного доступа по сети Ethernet задайте пароль. Этот пароль используется при установлении связи между контроллерами системы и программным обеспечением. Когда есть подозрение, что кто-то узнал старый пароль и подключается к контроллерам с целью управления ими, вводится новый.

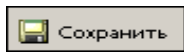
Для ввода нового пароля:

- Щелкните на кнопке **Изменение пароля** —



- В открывшемся окне введите новый пароль и подтвердите его, продублировав в нижнем поле ввода.



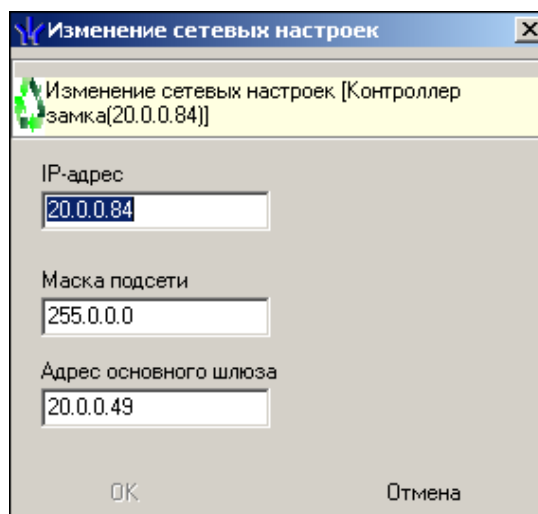
- Щелкните на кнопке «ОК».
- Сохраните данные щелчком на кнопке  в основном меню Консоли управления. Новый пароль будет сохранен.

Изменение сетевых настроек

Каждый контроллер имеет свои собственные настройки в сети, что упрощает их поиск, подключение друг к другу, обеспечивает связь между ними.

Для изменения сетевых настроек:

1. Выделите контроллер, чьи сетевые настройки подлежат изменению.
2. Отключите его.
3. Щелкните на кнопке **Изменение сетевых настроек** — . Откроется окно:



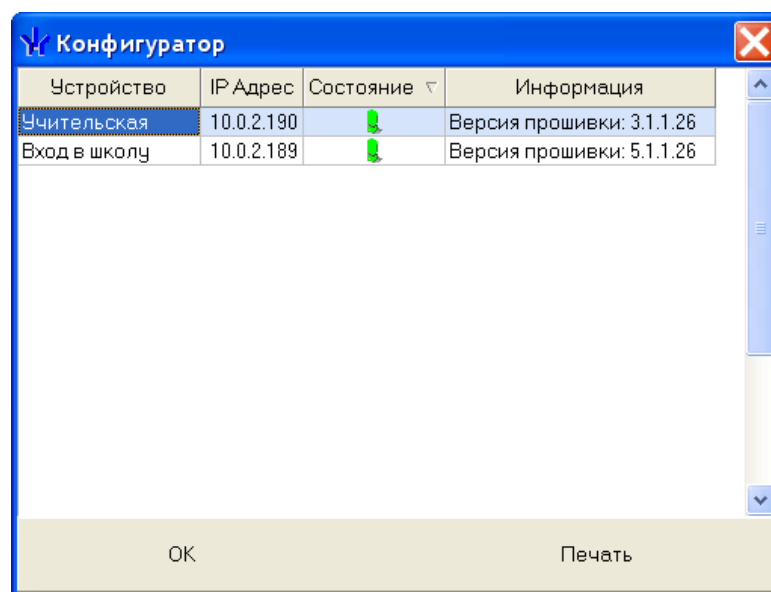
Произведите изменения.

Щелкните на кнопке «**ОК**», а затем передайте измененные параметры в аппаратуру с помощью кнопки **Передать измененные параметры** — . Сетевые настройки изменятся.

Получение информации о версиях прошивок

В системе PERCo-S-20 существует возможность обновлять версии прошивок контроллеров. Для получения текущих версий прошивок нажмите кнопку

Откроется окно:



Для закрытия окна щелкните на кнопке «**ОК**».

Кнопка **Печать** выведет на экран окно предварительного просмотра результатов выполнения команды:

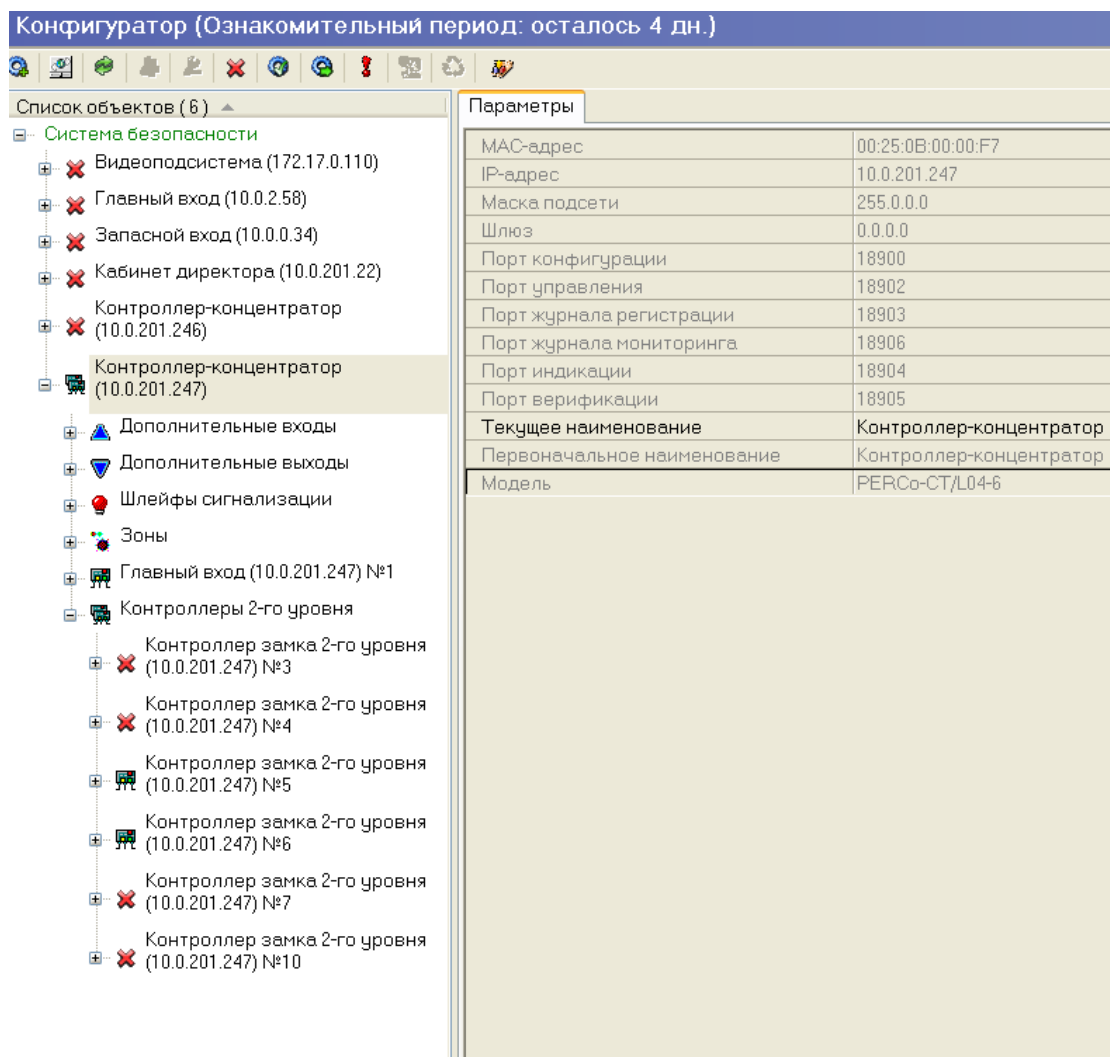
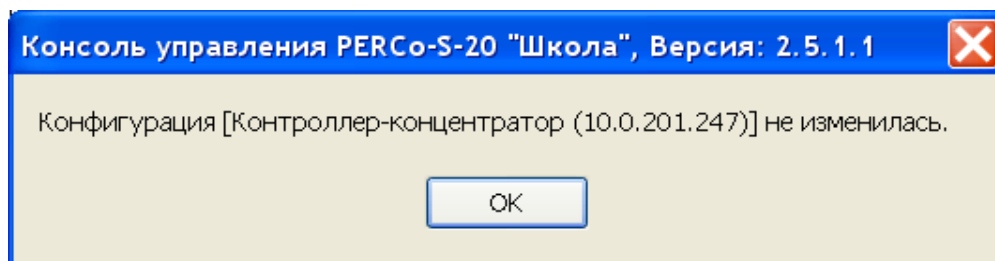
Результат выполнения команды

Контроллер	IP Адрес	Состояние	Информация
Учительская	10.0.2.190	Выполнено	Версия прошивки: 3.1.1.26
Вход в школу	10.0.2.189	Выполнено	Версия прошивки: 5.1.1.26

Изменение конфигурации контроллеров типа PERCo CT/L04

Кнопка позволяет обновить конфигурацию Контроллера-концентратора PERCo CT/L04, если были изменения в составе контроллеров 2 уровня то после проведения обновления конфигурации будет выдано сообщение.

Или если конфигурация не изменилась то:

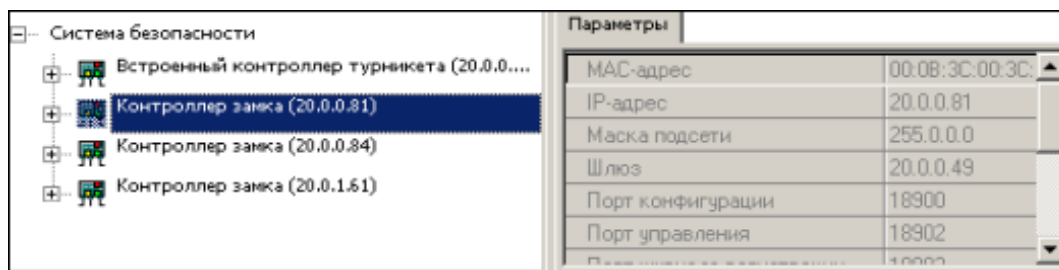


Изменение параметров аппаратуры

Любое устройство, входящее в состав системы, имеет те или иные параметры своего функционирования. Список устройств, входящих в состав системы, отображается в рабочем окне раздела Конфигуратор. При выборе любого из устройств на вкладке **Параметры** отображаются параметры выбранного устройства или его составляющих элементов.

Для просмотра параметров устройства выделите устройство.

В правой части рабочего окна отображается вкладка **Параметры**:

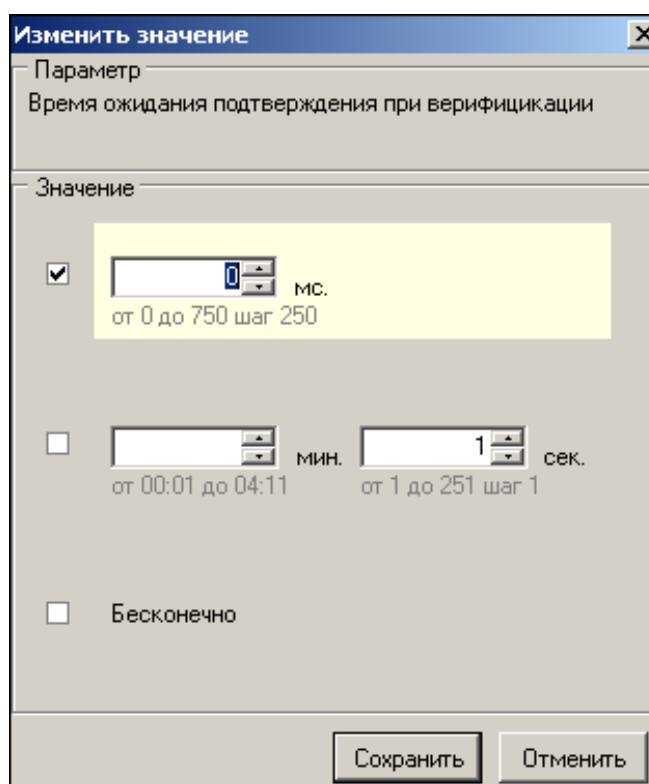


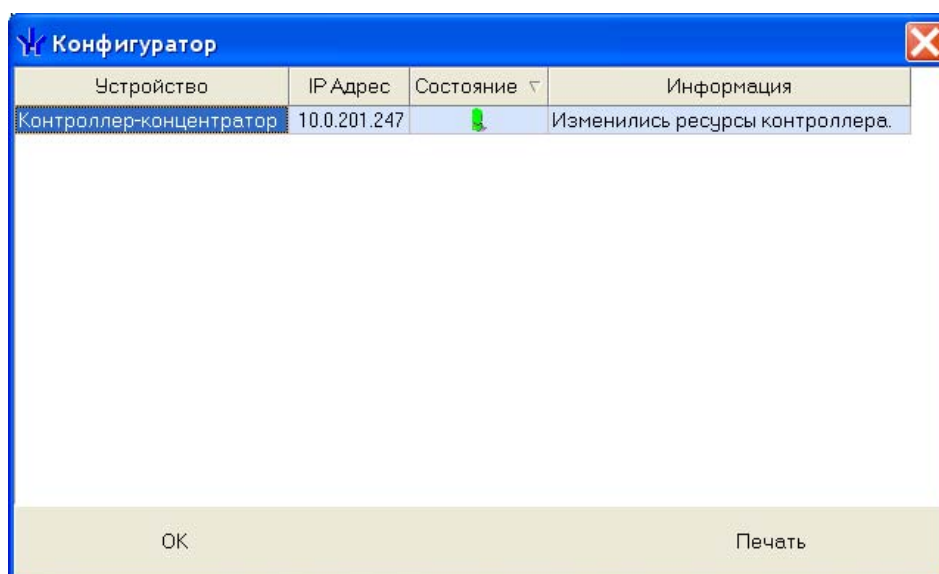
Редактирование параметров возможно только у составляющих элементов устройств. Изменение параметров осуществляется путём выбора нужной ячейки со свойством объекта и вводом нового значения:

Если возможен выбор из ограниченного числа вариантов, выберите нужный вариант



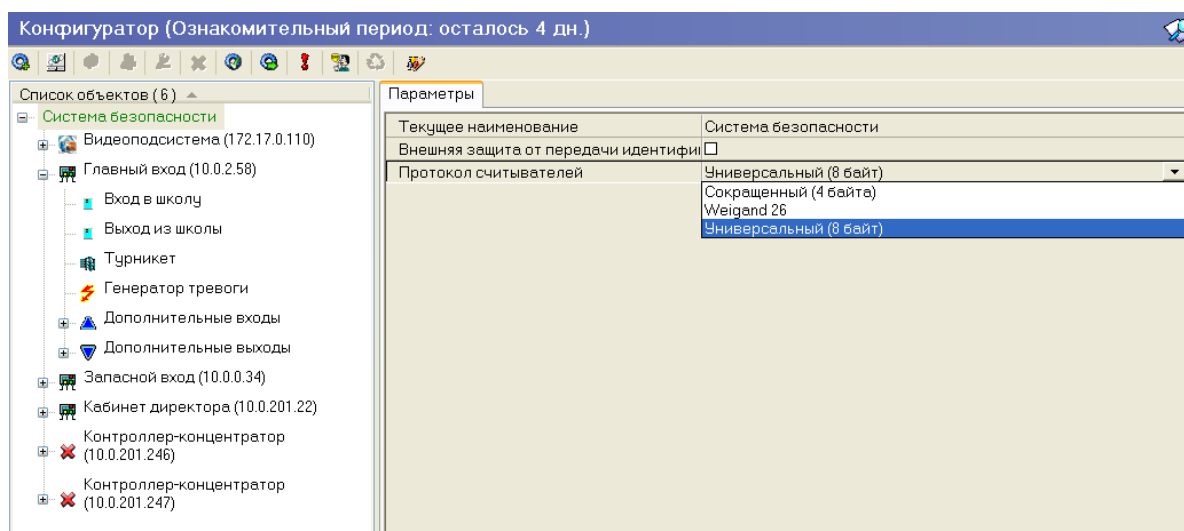
Если параметр числовой — введите необходимое значение вручную, либо щелкните на кнопке  и введите значение при помощи клавиатуры или кнопок полосы прокрутки в открывшемся окне изменения значений:





Устройство и его элементы после изменения параметров отобразятся в списке шрифтом зеленого цвета, напоминая, что внесенные изменения не переданы в аппаратуру.

Изменение протокола считывателей



Изменение протокола считывателей устанавливает в контроллерах доступа режим считывания идентификаторов карт доступа:

1. Универсальный(8 байт) - наиболее общий и правильный режим считывания, при установке данного режима считывается номер полностью, размерностью до 64 бит, то есть в нем уместятся все форматы карт E-marin.
- 2 Weigand 26 - 2 контрольных бита четности и нечетности находящихся соответственно в старшем и младшем бите и 3 байта номера из которых старший байт принять считать семейством максимальное значение 255 и 2 младших номером максимум 65535.
- 3.Сокращенный (4 байт) - частный случай более общего 8 байтового режима считывания

При выборе протокола Weigand 26 считыватель контроллера будет приводить номер карты к формату Weigand 26, вне зависимости от истинного формата карты. Если затем изменить протокол на универсальный то если карта истинно содержит Weigand 26, то с её доступом ничего не изменится, но если её истинный формат другой (не Weigand 26), то данная карта не получит доступа.



ПРИМЕЧАНИЕ

Изменение протокола считывателей лучше всего провести после монтажа оборудования и в дальнейшем при эксплуатации не менять.

ОПИСАНИЕ ПАРАМЕТРОВ ВИДЕОПОДСИСТЕМЫ

Подсистема видеонаблюдения единой системы безопасности PERCo-S-20 состоит из следующих элементов:

- ✓ **Сервер видеонаблюдения** - раздел, предназначенный для обеспечения работы системы безопасности с камерами видеонаблюдения, ведения архива видеонаблюдения.
- ✓ **Видеоконтроль/Видеонаблюдение PERCo-SM12 Видеонаблюдение** – раздел, предназначенный для отображения видеоинформации с камер видеонаблюдения на рабочем месте оператора. Управления видеокамерами, просмотра видеоархива.
- ✓ **Верификация/идентификация PERCo-SM09 Видеоидентификация, Прием посетителей PERCo-SM10 Прием посетителей** – разделы, предназначенные для контроля и управления входом в помещения, контролируемые подсистемой контроля доступа с одновременным отображением и записью видеоинформации с камер видеонаблюдения.

Для функционирования этих программных модулей необходимо описать параметры работы всей подсистемы видеонаблюдения. Описание настроек работы сервера видеонаблюдения приведено в соответствующей главе данного руководства.

Ниже приводится описание параметров работы видеоподсистемы и видеокамер.

Видеоподсистема

В данном случае под видеоподсистемой понимается программный модуль Сервер видеонаблюдения, который отображается в дереве устройств системы:

The screenshot shows a software interface with two main panels. The left panel, titled 'Список объектов (31)', displays a tree structure under 'Система безопасности'. It includes a 'Видеоподсистема (172.17.1.5)' which contains several cameras: 'AXIS 241S 90 (192.168.1.90)', 'AXIS 212 PTZ 89 (192.168.1.100)', 'Mobotix_mx10-2-161-114 74 (192.168.1.74)', 'Mobotix_mx10-3-32-5 75 (192.168.1.75)', and 'Kingwave kw3720 31 (192.168.1.31)'. The right panel, titled 'Параметры' and 'События', shows a table of parameters for the selected video subsystem.

Параметры	События
MAC-адрес	00:18:F3:83:72:5F
IP-адрес	172.17.1.5
Маска подсети	255.0.0.0
Порт конфигурации	20900
Порт управления	20902
Порт журнала мониторинга и регистрации	20903
Текущее наименование	Видеоподсистема
Первоначальное наименование	Видеоподсистема
Модель	PERCo-VS01
Частота кадров при записи для "Прозрач	60 кадр/мин.

В качестве параметров работы должны быть заданы:

- **Текущее наименование** - название, которое будет отображаться в дальнейшем в журналах мониторинга и регистрации.
- **Частота кадров при записи для «Прозрачного здания»** - параметр, указывающий количество записываемых кадров в минуту. Этот параметр имеет смысл только в случае использования программного модуля Прозрачное здание. И влияет на частоту записываемых кадров с камер видеонаблюдения, у которых установлен параметр «Использовать в прозрачном здании». При установке этого параметра необходимо учитывать трафик локальной сети. Рекомендованное значение не более 1 кадра в секунду.

Может быть задано только наименование, которое будет отображаться в дальнейшем в журналах мониторинга и регистрации.

Также в панели параметров отображаются не изменяемые параметры работы сервера видеонаблюдения.

Видеокамеры

Ниже приводится описание параметров функционирования камер видеонаблюдения, необходимых для их функционирования в системе безопасности PERCo-S-20.

В зависимости от типа используемой видеокамеры, меняется и список ее параметров.

Параметры События	
IP-адрес	192.168.1.90
Текущее наименование	AXIS 241S 90
Первоначальное наименование	AXIS 241S 90
Порт	80
Порт стоп-кадра	80
Логин пользователя	root
Пароль пользователя	xxxxxxxxxx
+ Детектор движения	
Частота кадров при записи	0 кадр/сек.
Продолжительность записи по команде от	0 сек.
+ Аудио-режимы	
+ Видео-режим	Режим "Unicast"

- **Текущее наименование** – параметр, задающий мнемоническое наименование выбранной камеры видеонаблюдения. Введенной значение будет использоваться в журналах мониторинга и регистрации.
- **Порт, Порт стоп-кадра** – параметры, указывающий номер порта, используемый для связи с выбранной камерой. Более подробная информация представлена в технической документации на выбранную виде камеру.
- **Логин пользователя, Пароль пользователя** – параметры, задающие имя и пароль пользователя, от имени которого будет осуществляться подключение к выбранной видеокамере. Задание имени пользователя и пароля необходимо для предотвращения доступа к видеокамере других пользователей.
- **Детектор движения** — параметры, определяющие продолжительность записи и порт, имеющие отношение к детектору движения.
- **Частота кадров при записи** – параметр, задающий частоту записываемой видеоинформации при получении команды **Начать запись**.
- **Продолжительность записи** – время, в течение которого видеосервер будет осуществлять запись с выбранной камеры при поступлении команды «Начать запись». Команда о начале записи может быть подана в двух случаях: Оператором системы из программных модулей Мониторинг и Центральный пост; Как результат выполнения заданной реакции системы на произошедшее событие.
- **Аудио-режимы** — параметры режима работы видеокамеры. Наличие режима Downstream позволяет записывать и воспроизводить звук, полученный со встроенного микрофона камеры. Если этот режим выбран, необходимо включить передачу аудио и выбрать формат данных в веб-интерфейсе камеры.
- **Видео-режим** - параметры режима работы видеокамеры. Наличие того или иного режима зависит от типа камеры, версии sdk и прошивки камеры.

Http — в этом режиме камера работает через протокол http в формате mjpeg. В этом режиме камера ограничивает количество подключений (Ограничения ресурсов используемой камеры)

Unicast — в этом режиме камера работает либо через протокол RTSP/RTP/RTCP в формате mpeg4 или по нестандартному протоколу в формате mpeg4, поддерживаемому камерой. В этом режиме количество подключений также ограничено ресурсами камеры.

Multicast - в этом режиме камера работает либо через протокол RTSP/RTP/RTCP в формате mpeg4, либо по нестандартному протоколу в

формате mpeg4, поддерживаемому камерой. В отличие от Unicast, количество подключений к камере в этом режиме неограничено.

Tunnelled — режим туннелирования RTSP через http. Используется при невозможности подключения через Unicast, количество подключений также ограничено.

НАЗНАЧЕНИЕ ПРАВ ДОСТУПА ОПЕРАТОРОВ

Раздел Назначение прав доступа операторов предназначен для ведения списка операторов системы, установки для них пароля, оперативного управления их правами, выдачи для каждого из них прав на работу со всеми разделами программного обеспечения. Для активизации раздела щелкните на кнопке раздела Назначение прав доступа операторов. Рабочее окно раздела отобразится в основной части окна Консоли управления. Рабочее окно раздела Назначение прав доступа операторов состоит из следующих элементов:

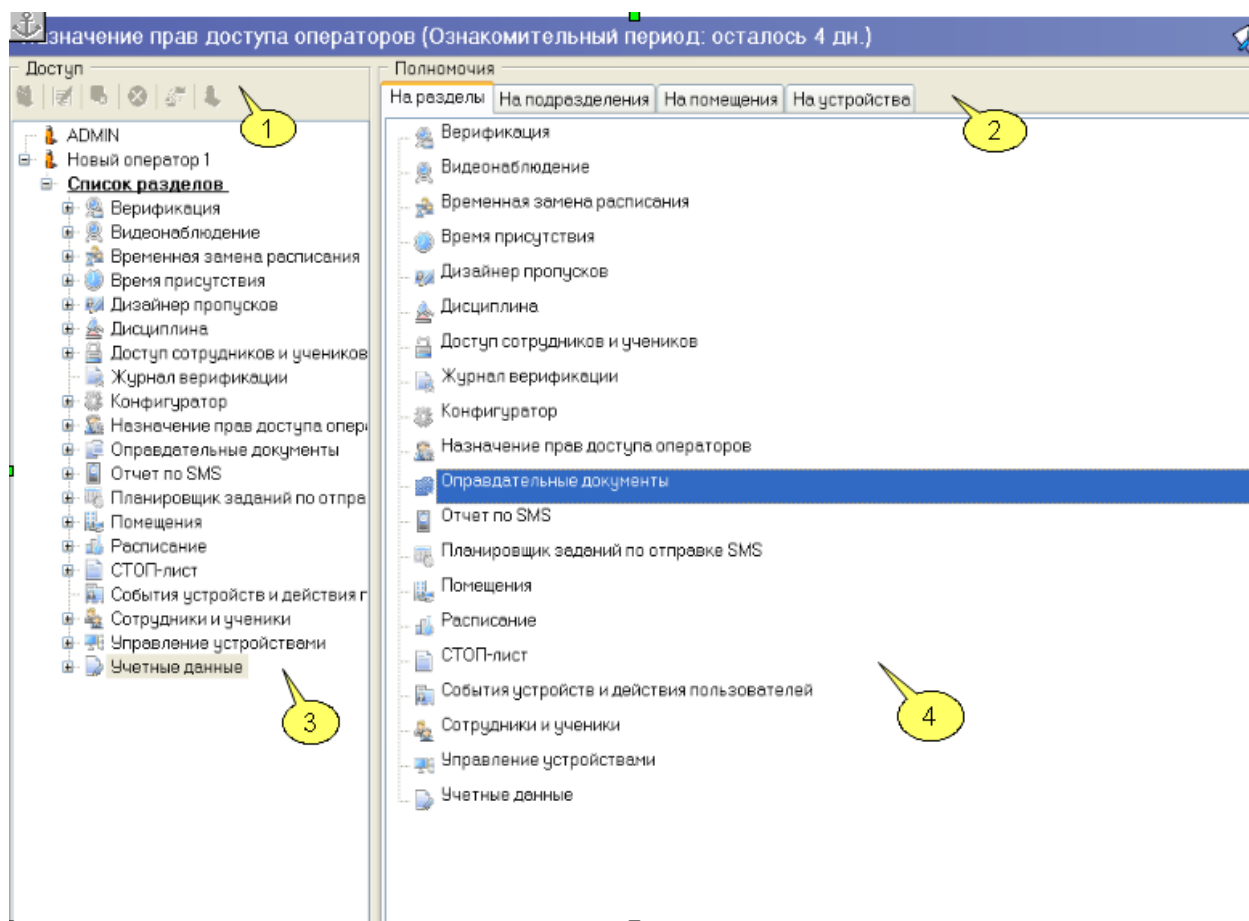


Рис. 5 Рабочее окно раздела Назначение прав доступа операторов

1. Функциональные элементы раздела Назначение прав доступа операторов



- 1 — **Добавить пользователя**
- 2 — **Редактирование данных пользователя**
- 3 — **Удалить пользователя**
- 4 — **Запретить доступ оператору**
- 5 — **Копирование прав**
- 6 — **Показать скрытых пользователей**

2. Вкладки рабочей области **Полномочия: На разделы, На подразделения, На помещения, На устройства.**
3. Список всех зарегистрированных пользователей с указанием прав каждого из них.
4. Рабочая область вкладок представлена в виде многостраничного блокнота с информацией о разделах ПО и объектах системы, на которые могут быть предоставлены права доступа операторам системы.

Ниже описываются функциональные возможности, предоставляемые системой пользователю раздела Назначение прав доступа операторов.

Добавление пользователя

Перед добавлением новых операторов необходимо подготовить соответствующий административный документ, который должен определять права каждого оператора по работе с системой безопасности. После составления этого документа можно приступить к вводу данных об операторах программного обеспечения.

Для добавления пользователя:

1. Щелкните на кнопке **Добавить пользователя** — . В нижней части рабочей области **Доступ** откроется дополнительная панель для ввода данных:



The screenshot shows a window titled "Доступ" (Access). At the top, there is a toolbar with several icons. Below the toolbar, there is a list of users: "ADMIN" and "маа". Below the list, there is a form to add a new user. The form has the following fields:

- Пользователь** (User): Text box containing "азб".
- Полное имя** (Full name): Text box containing "Алексеев Андрей борисович".
- Пароль** (Password): Text box containing "*****".
- Подтверждение пароля** (Password confirmation): Text box containing "*****".
- Дополнительная информация** (Additional information): Text box containing "охрана".
- Предоставить права администратора** (Grant administrator rights): Check box, which is checked.

At the bottom of the form, there are two buttons: "ОК" (OK) and "Отмена" (Cancel).

Укажите следующие данные на оператора (необходимым является только поле **Пользователь**, остальные – по желанию):

- **Пользователь** – в этой строке указывается имя пользователя, которое он будет вводить при запуске программного обеспечения.
- **Полное имя** – в этой строке указывается ФИО пользователя.
- **Пароль** – указывается пароль пользователя.
- **Подтверждение пароля** - указывается тот же самый пароль для избежания ошибки ввода.
- **Дополнительная информация** – в этой строке ввода можно ввести любую дополнительную информацию об операторе.

Флажок **Предоставить права администратора** позволяет предоставить вводимому пользователю права администратора системы безопасности. При этом этот пользователь будет иметь право доступа ко всему программному обеспечению, к изменению любых настроек системы и прав, а так же иметь возможность управлять любым устройством, входящим в систему безопасности.



ПРИМЕЧАНИЕ

Предоставить оператору права администратора может **только** администратор.

2. Для подтверждения введенных данных щелкните на кнопке «**ОК**».



ПРИМЕЧАНИЕ

В системе всегда присутствует предопределенный пользователь “ADMIN”. После установки системы необходимо задать ему пароль, по умолчанию пароль отсутствует. Этот пользователь или любой другой пользователь с правами администратора имеет доступ ко всем разделам программного обеспечения и возможность управления и изменения параметров всех устройств, входящих в систему безопасности.

Редактирование данных пользователя

Для редактирования данных пользователя:

1. Выделите пользователя, чьи данные необходимо отредактировать.
2. Щелкните на кнопке **Редактирование данных пользователя** — . В нижней части рабочей области **Доступ** откроется дополнительная панель для редактирования данных:



3. Для подтверждения измененных данных щелкните на кнопке «ОК».

Удаление пользователя

Для удаления пользователя:

- Выделите пользователя, которого необходимо удалить.
- Щелкните на кнопке **Удалить пользователя** —  . Откроется окно подтверждения:

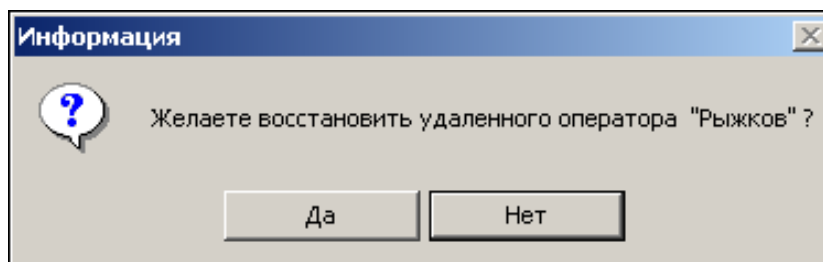
- Щелкните на кнопке «Да». Пользователь будет скрыт.
- Сохраните данные с помощью кнопки  **Сохранить** в основном меню Консоли управления.

Если пользователю были назначены права доступа, а его удалили по каким-либо причинам, то пользователь будет скрыт, а его права удалены.

Для отображения скрытых пользователей щелкните на кнопке **Показать скрытых пользователей** —  .

Для восстановления скрытых пользователей:

- Щелкните на кнопке **Восстановить пользователя** — . Откроется окно подтверждения:



- Щелкните на кнопке «**Да**». Пользователь будет восстановлен.
- Сохраните данные с помощью кнопки  **Сохранить** в основном меню Консоли управления.

Предоставление прав доступа оператору

Для предоставления прав доступа оператору выделите его мышью в списке операторов системы и выберите соответствующую вкладку в правой части рабочего окна.

Права доступа на разделы

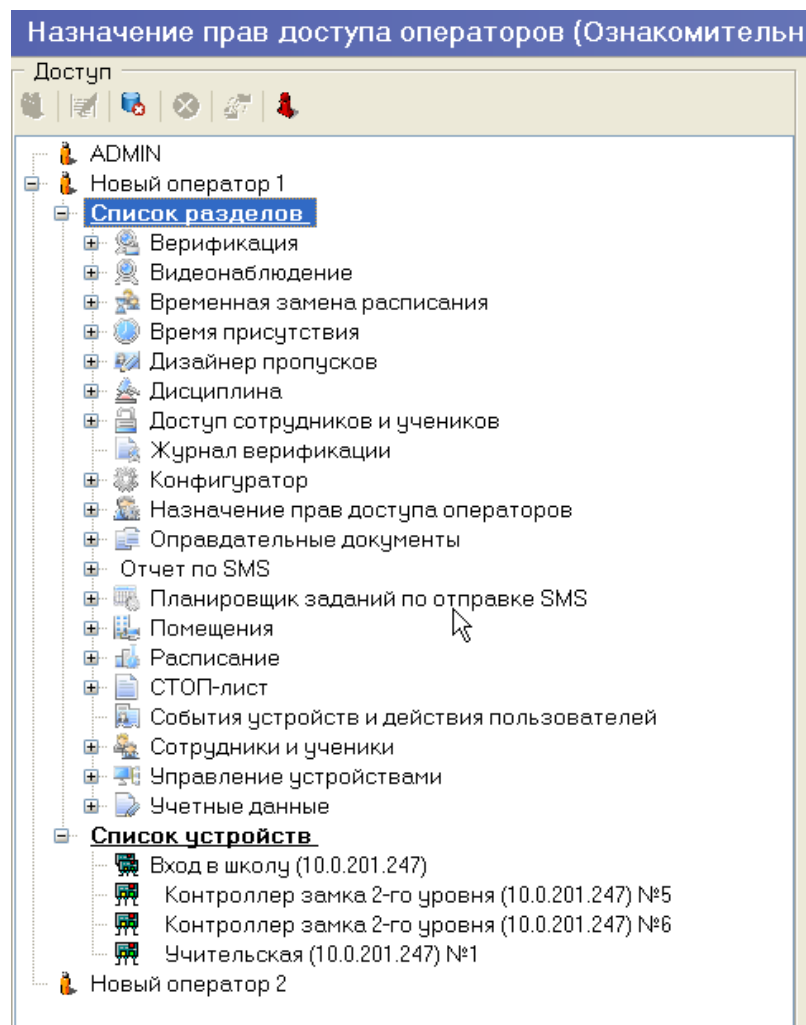
На вкладке **На разделы** представлен список всех разделов программного обеспечения, к которым может быть предоставлен доступ выбранному оператору.

Для предоставления доступа выберите необходимый раздел программного обеспечения в списке, и, не отпуская клавиши мыши, перетащите его на имя оператора, которому предоставляется доступ.

После этого название добавленного раздела программного обеспечения отобразится под оператором:

Перетаскивание названия раздела определяет, что данный оператор имеет право на вход в этот раздел и просмотр имеющейся там информации. Кроме этого для раздела могут быть указаны дополнительные права:

- **Право на изменение** — позволяет вносить и сохранять изменения в данные, предоставляемые этим разделом.
- **Право на передачу данных в аппаратуру** — позволяет оператору передавать измененные данные в устройства системы.



ПРИМЕЧАНИЕ

Возможно выделение сразу нескольких разделов: выделите группу разделов, удерживая клавишу **Shift** и не отпуская левую кнопку мыши, либо щелкайте по отдельным разделам, удерживая клавишу **Ctrl**.

Для предоставления дополнительных прав необходимо установить метку у соответствующего права.

Права доступа на подразделения

Вкладка **На подразделения** позволяет указать список подразделений, информация о сотрудниках которых будет доступна этому оператору.

Порядок действий предоставления права оператору полностью аналогичен описанному выше (см. [Права доступа на разделы](#) выше). При этом при перетаскивании подразделения, имеющего вложенные подразделения, автоматически будут добавлены все вложенные подразделения.

Права доступа на помещения

Вкладка На помещения позволяет указать список помещений данного предприятия, в которые данный оператор сможет разрешать/запрещать доступ. И также устанавливать параметры этого доступа.

Порядок действий предоставления права оператору полностью аналогичен описанному выше (см. Права доступа на разделы выше).

Права доступа на управление устройствами

Вкладка На устройства дает возможность указать, какими именно устройствами, входящими в систему безопасности, будет разрешено управлять оператору.

Порядок действий предоставления права оператору полностью аналогичен описанному выше (см. Права доступа на разделы выше).

Запрет доступа пользователя

Для запрета доступа пользователя:

1. Выделите пользователя, которому необходимо запретить доступ.
2. Щелкните на кнопке **Запретить доступ оператору** — . Слева от пользователя отобразится значок .

Для восстановления доступа пользователя щелкните на этой же кнопке еще раз.



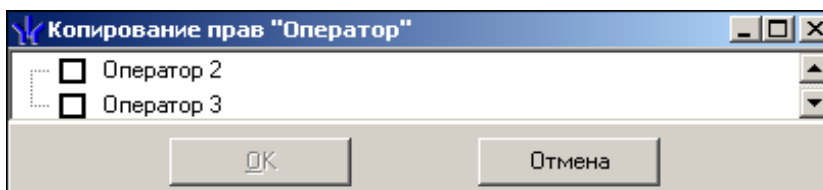
ПРИМЕЧАНИЕ

Запрет доступа, изменения списка доступных устройств, разделов, помещений и подразделений вступит в силу после начала нового сеанса пользователем, которому были внесены изменения.

Копирование прав

Для копирования прав:

1. Выделите пользователя, чьи права будут скопированы (права могут быть скопированы не полностью, а частично, например, права доступа только в один раздел или на один этаж).
2. Щелкните на кнопке **Копирование прав** — . Откроется окно:



3. Укажите, кому надо скопировать права, отметив флажки, и щелкните на кнопке «ОК». Права будут скопированы.

УПРАВЛЕНИЕ СЕРВЕРАМИ

Для управления сервером системы PERCo-S-20 и сервером баз данных перейдите по следующей ссылке (Пуск → Настройка → Панель управления → Центр управления PERCo-S-20 Школа):

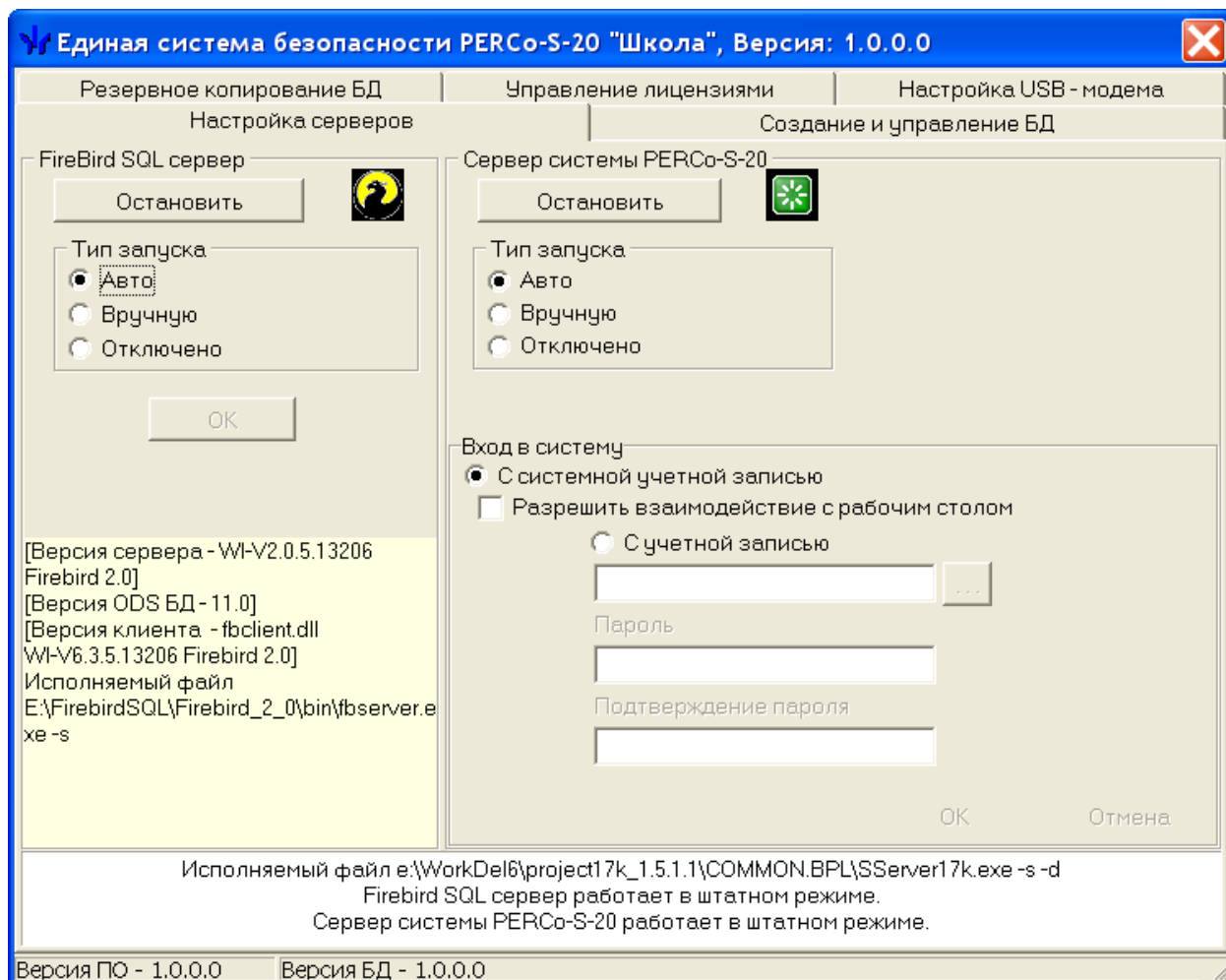


Рис. 6. Центр управления PERCo-S-20 Школа

Вход в систему в режиме, когда отмечен переключатель **С системной учетной записью**, позволяет настроить почтовую рассылку сообщений о создании резервных копий базы данных (см. п. [Резервное копирование БД](#)).

БАЗА ДАННЫХ

В качестве сервера БД в системе PERCo-S-20 «Школа» используется SQL-сервер Firebird 2.0. Он устанавливается вместе с ПО системы, тем не менее, сама база данных создается вручную.

Для создания и управления настройками базы данных системы PERCo-S-20 «Школа» предназначена вкладка **Создание и управление БД**:

Единая система безопасности PERCo-S-20 "Школа", Версия: 1.0.0.0

Резервное копирование БД | Управление лицензиями | Настройка USB - модема

Настройка серверов | **Создание и управление БД**

Расположение базы данных:
C:\temp\db\SCD17k.fdb

Расположение архивов базы данных:
C:\temp\db\

Учетная запись пользователя:
SYSDBA

Пароль пользователя:
XXXXXXXXXX

Настройка сервера системы и сервера Firebird

Порт данных	Порт FireBird
211	3050
Порт уведомлений	Время восстановления соединения (сек.)
411	30
Время конфигурации по одному сетевому интерфейсу (мин.)	
1	

Режим

☒ Изменение настроек

☐ Создание базы данных

Версия ПО - 1.0.0.0 | Версия БД - 1.0.0.0

- ✓ **Расположение базы данных.** В этой строке указывается путь к файлу БД. Данный путь может быть введен непосредственно в строке ввода или выбран при использовании кнопки, которая расположена справа от строки ввода.
- ✓ **Расположение архивов базы данных.** В этой строке указывается путь к каталогу, в котором будут размещаться архивные копии базы данных. Правила ввода пути аналогичны предыдущим.
- ✓ **Учетная запись пользователя.** Этот параметр задает имя пользователя, от которого будет осуществляться доступ к файлу базы данных.
- ✓ **Пароль пользователя.** Этот параметр задает пароль пользователя, от имени которого будет происходить обращение к файлу базы данных.
- ✓ **Настройки сервера системы и сервера FireBird** – параметры, определяющие значения портов ввода/вывода, которые используются программным обеспечением для связи между программными модулями и БД.
- ✓ **Время восстановления (сек)** - время, через которое Сервер системы попытается восстановить связь с любым контроллером системы в случае ее неожиданной потери.
- ✓ **Время конфигурации по одному сетевому интерфейсу (мин)** – предельный минимум времени, отведенный на конфигурацию по одному адресу и маске подсети. Пользователь может изменить его по своему усмотрению, но значение не может быть меньше предопределенного (1 мин).

Созданные базы данных



Щелкнув на иконке из Панели управления, запустите «Центр управления PERCo-S-20»

Убедитесь (см. Рис. 6), что Firebird SQL Server запущен. Информация об этом расположена в нижней части окна.

Для создания базы данных перейдите на вкладку **Создание и управление БД** (Рис. 7):

Выберите переключателем режим работы **Создание базы данных**. Заполните соответствующие поля.

Заполните параметры базы данных:

- ✓ Укажите путь к тому месту, где будет создан файл базы данных. Это путь к компьютеру, где был ранее установлен SQL-сервер Firebird 2.0. Папку, в которой вы создаете файл базы данных, для повышения безопасности не рекомендуется предоставлять в общее пользование. Если база находится на том же компьютере, что и сервер управления, вы можете выбрать путь с помощью кнопки , если нет, то кнопка будет неактивной, и вы должны ввести путь вручную.
- ✓ Укажите путь к архиву базы данных. Это путь к директории, где будут создаваться архивные копии файла базы данных. Имя самого файла базы данных и архива лучше не изменять. Имя директории может вводиться вручную (тогда это директория на компьютере, где находится SQL-сервер) или выбираться щелчком мыши на кнопке . В этом случае можно выбирать

директорию, к которой предоставлен общий доступ с любого компьютера сети. Если SQL-сервер запущен как сервис, то данному сервису должен быть предоставлен полный доступ к директории. Если SQL-сервер запущен как приложение, то учетной записи, под которой он запущен, должны быть предоставлены права на директорию.

- ✓ Введите имя пользователя, который будет создателем и владельцем файла базы данных (оставьте предопределенное).
- ✓ Введите пароль пользователя для доступа к БД (оставьте предопределенный).



ПРИМЕЧАНИЕ

Пользовательские имя и пароль указываются один раз при создании базы данных. Они не имеют отношения к реальным пользователям, которые получают доступ к БД из клиентских приложений.

После ввода всех характеристик нового файла баз данных щелкните на кнопке **Создание базы данных**.

После создания базы можно работать с любым разделом программного обеспечения системы PERCo-S-20. Поля данных на вкладке заполнятся введенными параметрами. И станут доступными следующие элементы управления (Рис. 8):

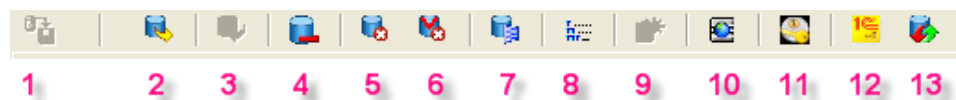


Рис. 8. Элементы управления базой данных

- 1 — Сохранение настроек базы данных
- 2 — Сохранение базы данных оптимизация и проверка целостности(см. «Сохранение базы данных»)
- 3 — Восстановление БД
- 4 — Удаление данных мониторинга
- 5 — Удаление данных по событиям
- 6 — Удаление данных по видеоидентификации
- 7 — Настройки сервера БД
- 8 — Оптимизация индексов
- 9 — Создание базы данных
- 10 — Обновление версии базы данных
- 11 — Восстановление предыдущего пароля устройств
- 12 — Настройка работы с 1С
- 13 — Проверка целостности БД

Сохранение настроек базы данных

Этот элемент управления позволяет сохранить изменения, внесенные в параметры базы данных.

Сохранение базы данных

Щелчком на кнопке **Сохранение базы данных оптимизация и проверка целостности** —  происходит создание полной резервной копии базы данных. Выбор места расположения резервной копии БД определяется на этапе создания (см. «[Создание базы данных](#)»). Однако резервные копии БД можно делать и в другом месте. Для внесения изменений выполните следующие действия:

- ✓ Выбирается имя компьютера, на котором установлен Сервер БД, т.е. указывается имя компьютера, где расположен SQL-сервер Firebird 2.0.
- ✓ Вводится путь к файлу базы данных. Необходимость менять путь к базе может возникнуть при переносе базы. Если “Центр управления серверами PERCO S-20” запущена на том же компьютере, где установлен SQL-сервер Firebird 2.0, то Вы можете выбрать путь с помощью кнопки , если нет, то кнопка будет неактивна, и Вы должны ввести путь вручную.
- ✓ Указывается директория, в которой сохраняются архивные файлы. Имя директории может вводиться вручную (тогда это директория на компьютере, где находится SQL-сервер) или выбираться щелчком на кнопке . В этом случае можно выбрать директорию, к которой предоставлен общий доступ с любого компьютера сети (не рекомендуется, т.к. замедляется создание архивов и их восстановление). Рекомендуется иметь второй HDD на компьютере с сервером Firebird и сохранять архивы на диск отличный от диска, где находится БД.
- ✓ Указывается пользователь, от имени которого создается база данных, и его пароль.

Восстановление базы данных из резервной копии

Восстановление данных из архива выполняется щелчком на кнопке **Восстановление БД** —

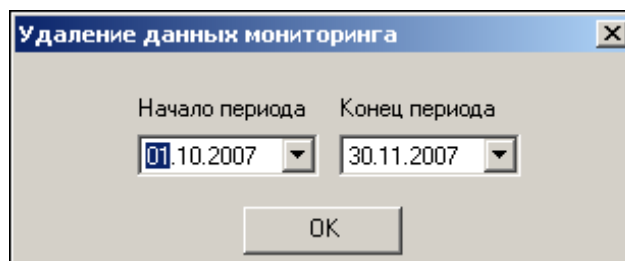


Сохраненная копия базы данных после восстановления имеет то же название, что и рабочая база, но с добавлением символа «#» в конце имени файла. После успешного выполнения команды восстановленная база становится рабочей.

При последующем восстановлении копия будет иметь тоже название, но уже без символа «#» на конце. После выполнения команды она также сразу станет рабочей. В результате, при нормальной работе существуют два файла базы данных (рабочая и предыдущая копия), а также набор архивных копий. Данная особенность создания резервных копий позволяет повысить надежность действий при восстановлении базы данных из архива и обеспечить безусловную работоспособность базы даже при наличии повреждений на диске.

УДАЛЕНИЕ ДАННЫХ МОНИТОРИНГА

Удалить данные мониторинга можно щелкнув мышью на кнопке —  :

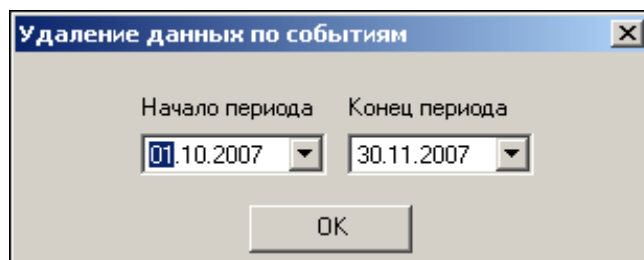


Выберите начало и конец периода мониторинга данных, подлежащих удалению. Подтвердите выбор щелчком на кнопке «**ОК**».

Проводите эти действия периодически. Это позволит уменьшить размер файла базы данных и ускорить работу программных модулей системы безопасности. Рекомендуется проводить эти действия один раз в месяц.

УДАЛЕНИЕ ДАННЫХ ПО СОБЫТИЯМ

Удаление данных по событиям становится возможным после щелчка на кнопке — 



Эти действия аналогичны действиям, описанным выше, за исключением того, что удаляются данные о событиях, зарегистрированных в системе и записанных в журнале регистрации. Рекомендуется проводить эти действия не реже одного раза в квартал после завершения формирования всех необходимых отчетов за удаляемый период.

НАСТРОЙКА СЕРВЕРА БАЗЫ ДАННЫХ

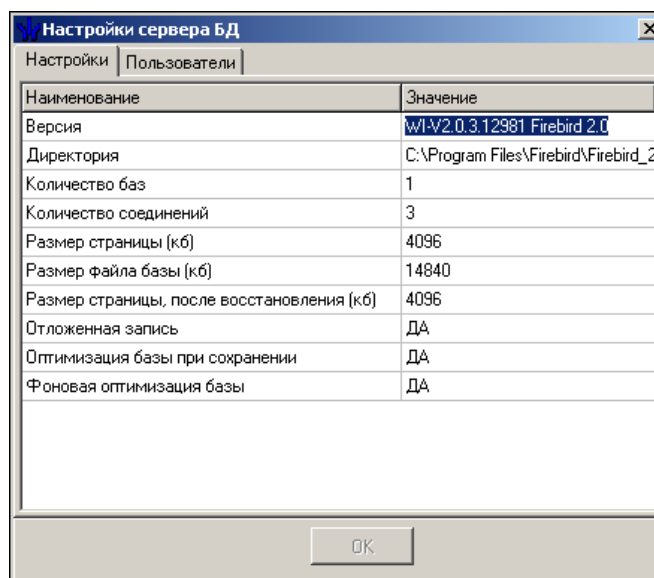
Окно **Настройки сервера БД** вызывается щелчком на кнопке — .

Окно **Настройки сервера БД** содержит две вкладки **Настройки** и **Пользователи**.

Вкладка **Настройки** включает следующие позиции:

- **Версия** SQL-сервера Firebird для сведения.

- **Директория** - место установки SQL-сервера Firebird.
- **Количество баз** – информационный параметр.
- **Количество соединений** – информационный параметр.
- **Размер страницы.** По умолчанию файл БД создается с размерами страницы 4096 байт.
- **Размер файла базы** - текущий размер файла базы данных системы PERCo-S-20.



- **Размер страницы, после восстановления.** При восстановлении БД, особенно при переносе на другой носитель, размер страницы может быть не кратным размеру кластера жесткого диска. Поэтому для оптимизации производительности рекомендуется устанавливать его кратным размеру кластера.
- **Отложенная запись.** Все изменения, затрагивающие данные на уровне файла базы данных, происходят с участием системного кэша, расположенного в памяти компьютера, что ускоряет файловые операции. Однако при сбоях компьютера, отключении питания и т.п. данные могут пропасть. Для повышения надежности сохранения оперативных данных можно отключить данный параметр, установив «Нет», при этом скорость операций с БД уменьшится.
- **Оптимизация базы при сохранении.** Данный параметр управляет необходимостью оптимизации БД (см. ниже «Фоновая оптимизация») при сохранении резервной копии БД.
- **Фоновая оптимизация базы.** При работе SQL-сервера создаются разные версии записей. При режиме «Да» они чистятся самим сервером, однако это замедляет его основную деятельность. Следует учесть, что сборка «мусора» происходит при сохранении базы данных, которое рекомендуется делать ежедневно. Поэтому рекомендуется выбирать режим «Нет».

На вкладке **Пользователи** предоставляется возможность изменить пароль администратора БД. Рекомендуется заменить пароль «masterkey», являющийся общеизвестным, на пароль известный только администратору системы (пароли регистрозависимы).

Оптимизация индексов базы данных

Оптимизация индексов осуществляется щелчком на кнопке  (рекомендуется проводить раз в неделю). Это действие позволяет оптимизировать работы программного обеспечения с базой данных.

Обновление версии базы данных

Обновление версии базы данных производится только в случае получения обновления для программного обеспечения. Подробные инструкции по проведению обновления приводятся в сопроводительной документации на обновленную версию.

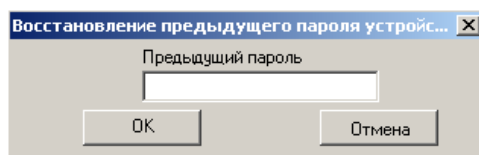
Восстановление предыдущего пароля устройств

Восстановление предыдущего пароля устройств может потребоваться в следующей ситуации:

После установки пароля и нормального функционирования системы, вы создали резервную копию БД. После этого вы сменили пароль для связи с устройствами системы и передали параметры. После этого вы восстановили БД из резервной копии.

В результате этих действий в программном обеспечении будет использоваться пароль, сохраненный до этого в БД, а в контроллерах системы будет использоваться пароль, установленный ранее. В этой ситуации программное обеспечение не сможет подключиться к контроллерам системы.

Для решения этой проблемы воспользуйтесь кнопкой **Восстановление предыдущего пароля устройств** — , расположенной в панели функциональных элементов. Щелчок на ней открывает диалоговое окно, в котором указывается пароль, введенный ранее (пароль установленный на данный момент в контроллерах системы). Щелкните на кнопке «ОК» в подтверждение ввода:

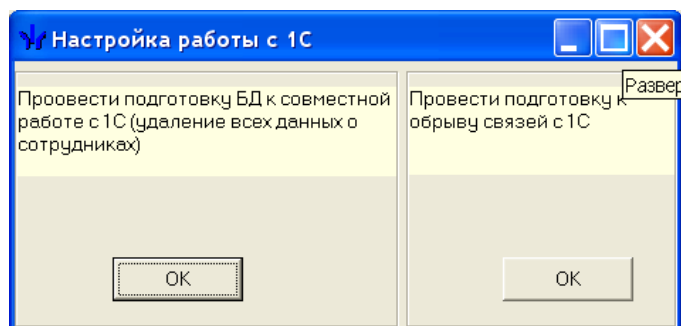


ПРИМЕЧАНИЕ

При восстановлении пароля все «Консоли управления» должны быть закрыты.

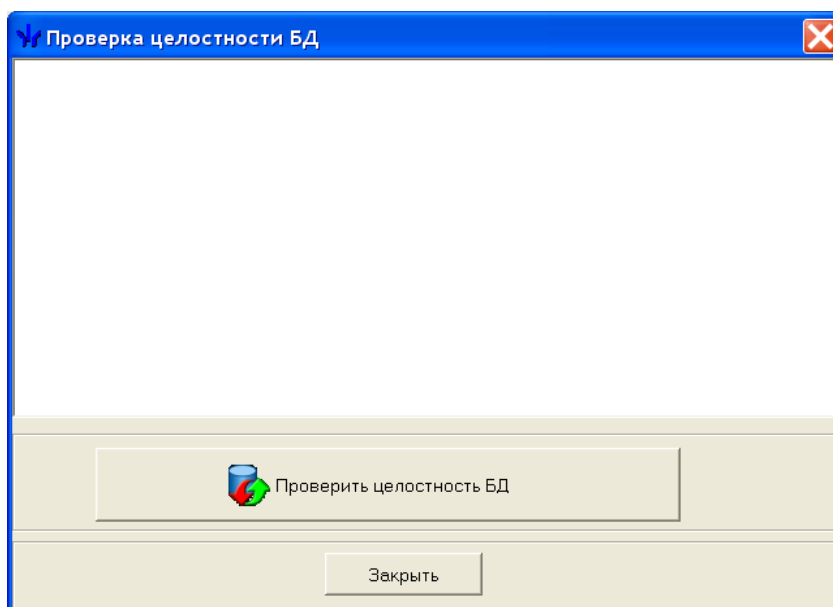
После задания нового пароля завершите работу с «Центром управления серверами». Запустите «Консоль управления» с установленным модулем Конфигуратор и передайте измененные параметры в контроллеры системы.

Настройка работы с 1С

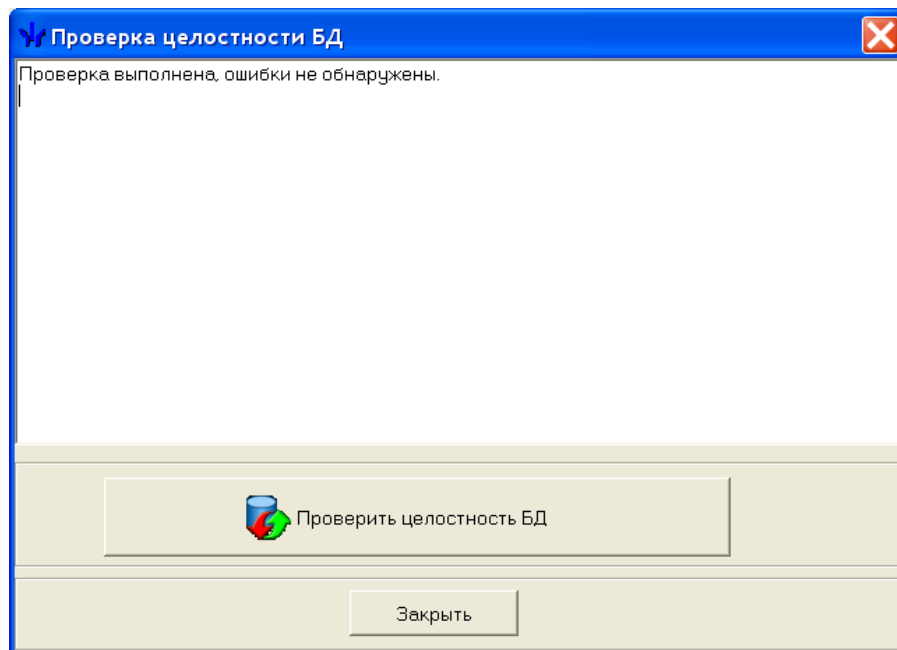


Удаление данных о сотрудниках приведёт к тому, что в базе PERCo будут оставлены только данные о аппаратуре, а данные о сотрудниках и их картах доступа будут удалены. Обрыв связей с 1С означает удаление из базы PERCo всех идентификаторов связи с 1С.

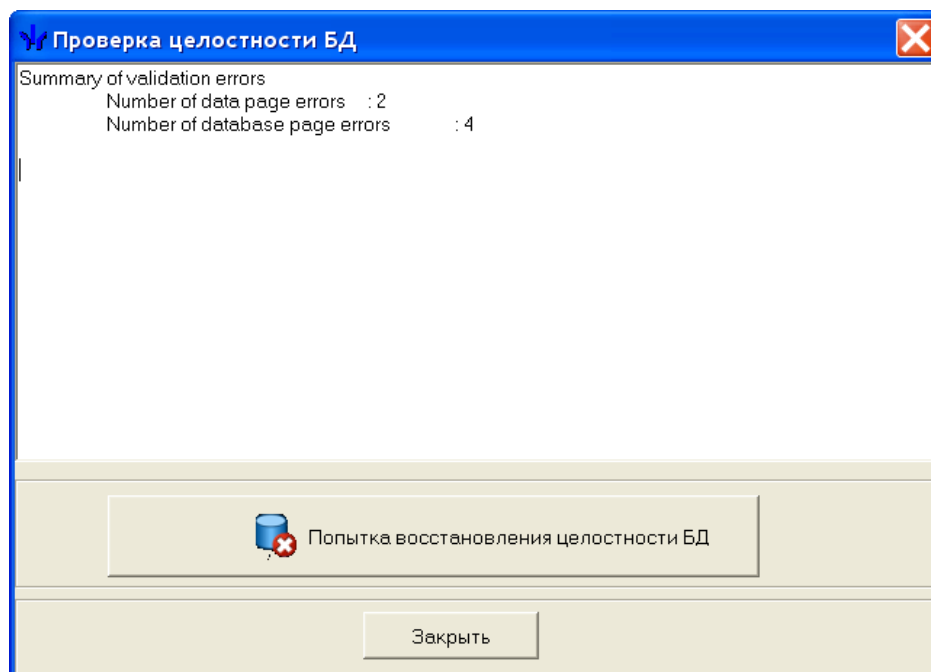
Проверка целостности БД



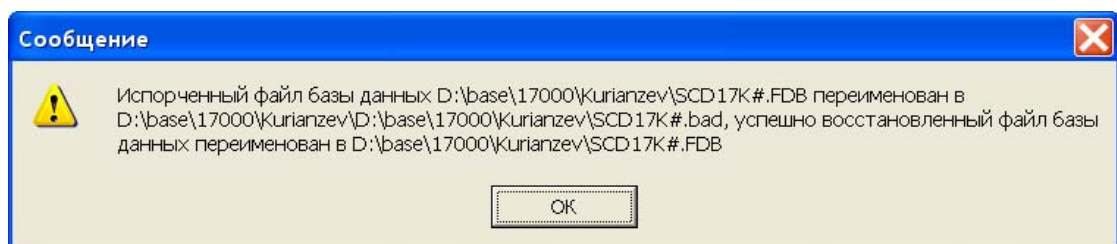
После нажатия на кнопку «Проверьте целостность БД» будет произведена проверка БД в случае отсутствия ошибок появится надпись.

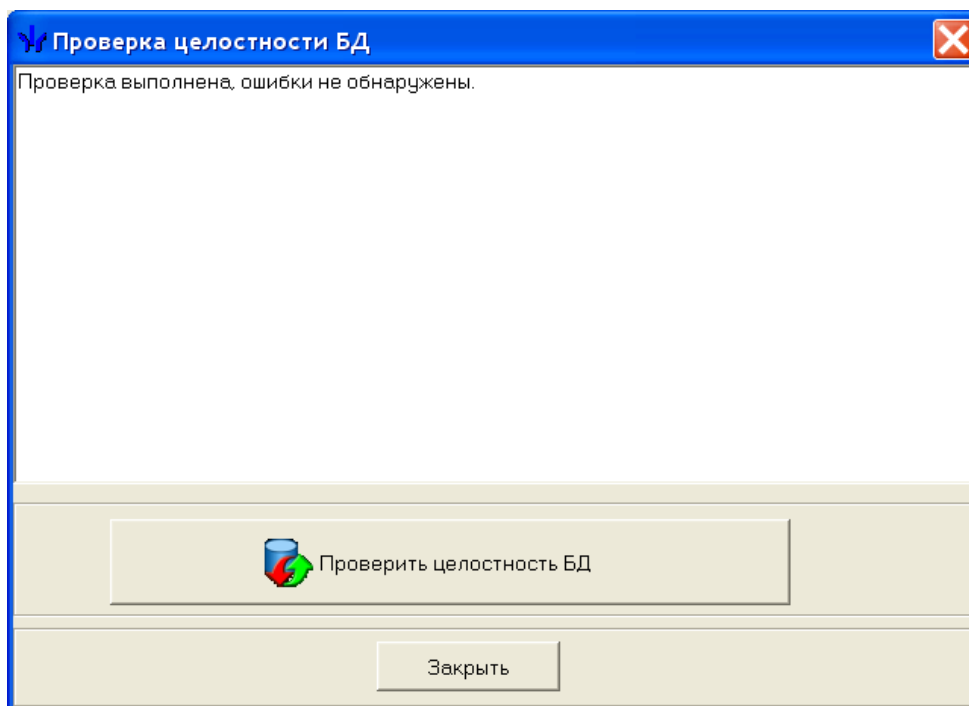


Иначе:



После нажатия на кнопку «Попытка восстановления целостности» в случае успешного восстановления появится сообщение





Резервное копирование БД

Одной из основных проблем обслуживания информационных систем является своевременное создание резервных копий базы данных. К сожалению, сбои в работе персональных компьютеров, жестких дисков не редкость.

Для обеспечения целостности базы данных и своевременного создания резервных копий программное обеспечение единой системы безопасности PERCo-S-20 предоставляет возможность по автоматизации этого процесса. На вкладке **Резервное копирование БД** модуля управления сервером системы Вы можете создать расписание, по которому будут автоматически создаваться резервные копии БД.

Резервная копия БД будет сохраняться в каталоге, указанном в строке **Расположение резервных копий базы данных** на вкладке Создание и управление БД данного модуля.

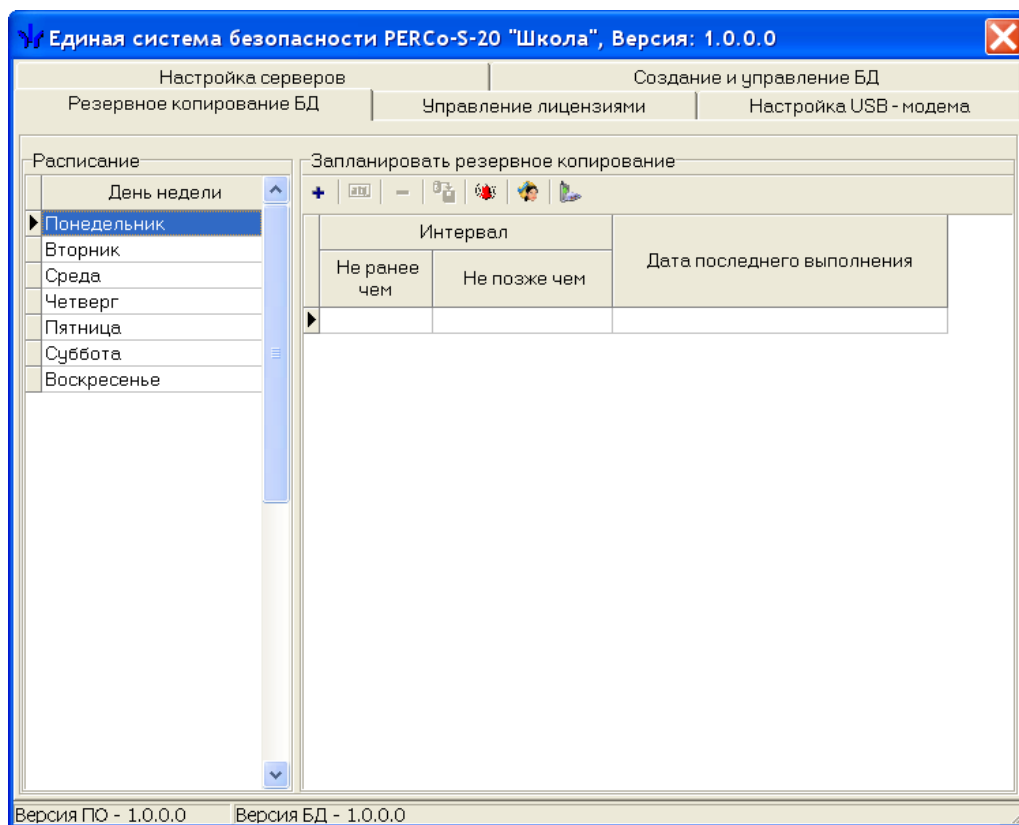
Для создания расписания выберите день недели и щелкните на кнопке . В нижней части окна откроется панель ввода:

В этой панели укажите интервал времени, в течение которого сервер системы проведет создание резервной копии БД. При условии работы системы в круглосуточном режиме рекомендуется установить этот интервал в ночное время.

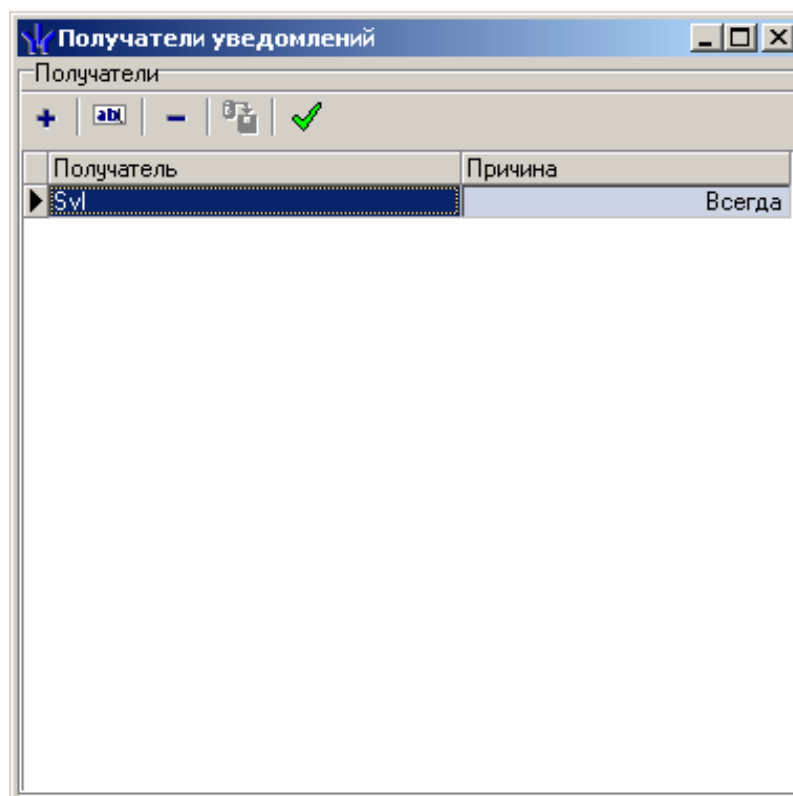
После завершения ввода временного интервала щелкните на кнопке «ОК» и сохраните внесенные данные щелчком на кнопке **Сохранение расписания** — .

Для изменения временного интервала используйте кнопку , для удаления - кнопку





При создании резервной копии базы данных существует возможность рассылки уведомлений о результатах выполнения. Для задания списка рассылки по сети воспользуйтесь кнопкой . Щелчком на ней открывается диалоговое окно, отображающее текущее состояние списка рассылки:



В нем отображается имя получателя уведомления и причина, по которой будет отправляться данное уведомление.

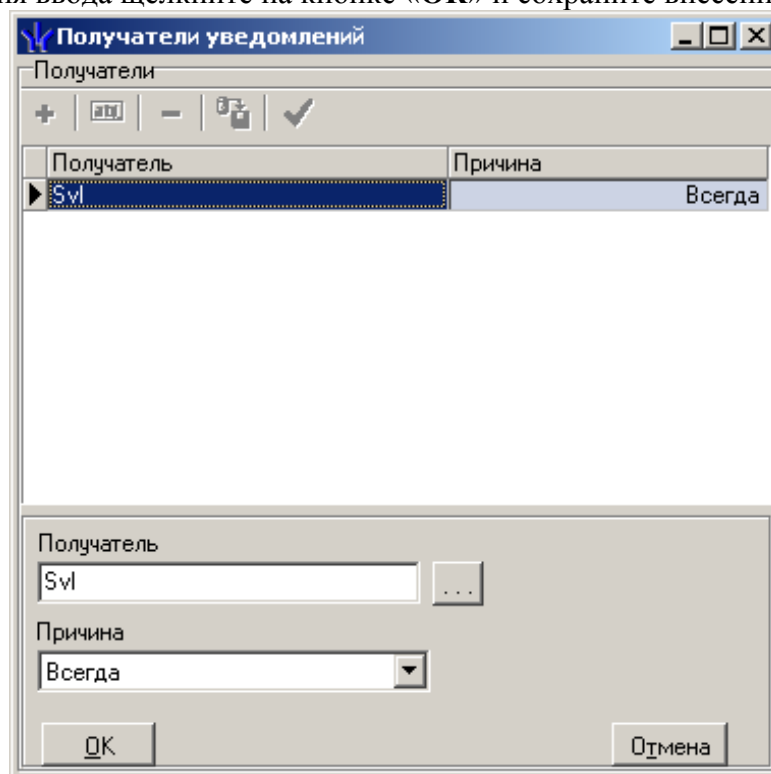
Кнопка  позволяет протестировать работу данной функции. Щелчком на этой кнопке выделенному сотруднику отправляется тестовое сообщение.

Для добавления нового получателя уведомлений используйте кнопку . Щелчком на ней в нижней части окна открывается панель ввода.

В этой панели введите имя компьютера, на которое будет отправлено сообщение и причину отправки, которая выбирается из списка. Доступны два варианта:

- **Всегда** – данное сообщение будет отправляться всегда, вне зависимости от результатов выполнения действий по созданию архивной копии.
- **В случае ошибки** – сообщение будет отправляться только в случае, если программное обеспечение не может создать резервную копию базы данных.

После завершения ввода щелкните на кнопке «ОК» и сохраните внесенные изменения.



Кнопкой **Настроить почтовую рассылку уведомлений** —  открывается окно настройки рассылки по электронной почте уведомлений о создании резервной копии БД.

Адресная книга

Отправитель

Адрес SMTP сервера (smtp.yandex.ru)
smtp.yandex.ru

Адрес отправителя (addr@yandex.ru)
hat@yandex.ru

Пользователь (addr@yandex.ru)
hat@yandex.ru

Пароль
xxxxxx

Получатели

Получатель	Адрес получателя	Когда посылать
Крюкова	kryukova@perco.ru	Всегда

Функциональные элементы окна настройки почтовой рассылки уведомлений аналогичны описанным выше функциональным элементам окна настройки рассылки по сети.

Кнопкой Настройка СМС рассылка  — открывается окно настройки рассылки СМС уведомлений о создании резервной копии БД.

Список телефонов для рассылки SMS

Код страны	Код региона	Номер телефона	Когда посылать
8	911	9991744	В случае ошибки

1/1

Получатель SMS

Код страны: 8 Код региона: 911 Номер телефона: 9991744 Когда посылать: В случае ошибки

OK Отмена

Функциональные элементы окна настройки почтовой рассылки уведомлений аналогичны описанным выше функциональным элементам окна настройки рассылки по сети.

Настройка USB – Модема

Для использования модема при посылки уведомлений сохранения базы или рассылки SMS-сообщений при предъявлении карты доступа или иного события или состояния устройств, необходимо предварительно его настроить. В качестве модема может выступать обычный сотовый телефон с встроенным модемом и возможностью подключением через USB порт компьютера, для рассылки уведомлений о сохранение данных его должно хватить, для массовой рассылки на десятки и сотни номеров необходимо использовать USB-модем.

Порядок настройки:

- Внимательно прочитать документацию по установке модема и установить ПО в соответствии с рекомендациями производителя.(при корректной установке у вас в Панель управления-Телефон и модем должна появится запись о установленном модеме)
- Запустить «Центр управления PERCo S-20» перейти на вкладку «Настройка USB-модема» и заполнить данные
- PIN код вводить нужно только если ваша SIM карта защищена.
- Записывать команды модема в лог файл необходимо при возникновении ошибок при использовании модема, для отсылки лога компании PERCo soft@perco.ru.
- Номер SMS-центра выясняется у оператора поставившего вам модем.
- Номер получателя вводится для проверки правильности настроек модема.

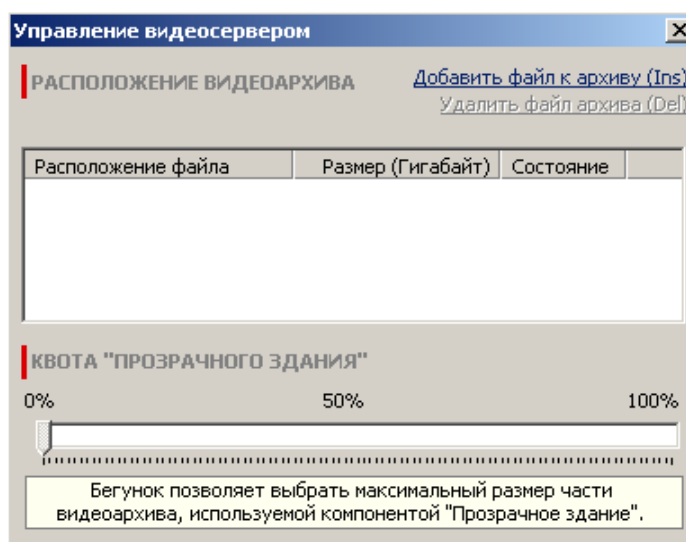
После завершения ввода настроек станет доступна кнопка отправить, нажмите на неё для проверки корректности настроек, при корректном вводе Получатель SMS должен получить SMS с набранным текстом.

СЕРВЕР ВИДЕОНАБЛЮДЕНИЯ

Сервер видеонаблюдения представляет собой программный модуль, предназначенный для создания систем Видеонаблюдения, Прозрачное здание и Верификация / Видеоидентификация.

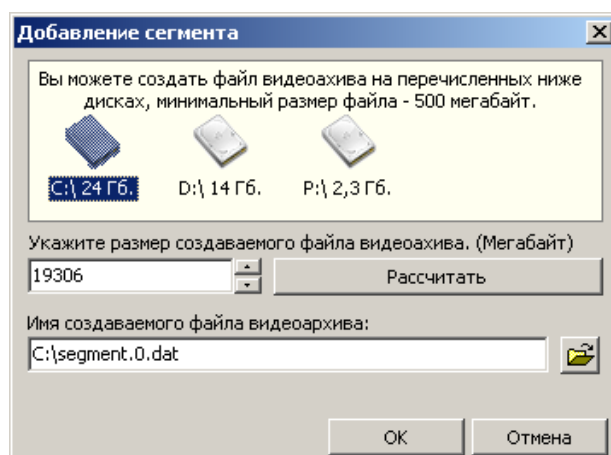
Для управления сервером видеонаблюдения PERCo-S-20 запустите Панель управления

Windows (Пуск → Настройка → Панель управления), щелкните на значке  :



В этом окне задайте место расположение файла видеоархива, в котором сервер видеонаблюдения будет сохранять видеoinформацию.

Для добавления файла видеоархива щелкните на [Добавить файл к архиву \(Ins\)](#) :



В открывшемся диалоговом окне выберите логический диск, на котором будет храниться файл видеоархива. Ниже программа выводит размер предполагаемого файла. Кнопка

Рассчитать позволяет определить какое количество камер и длительность записи будет возможно сохранить в этом файле.



ПРИМЕЧАНИЕ

Архив системы Видеонаблюдения имеет циклическую структуру. После заполнения старая информация будет автоматически перезаписываться!

Система позволяет создать несколько файлов видеоархива, расположенных на разных дисках.

Для удаления файла видеоархива выделите его в списке файлов:



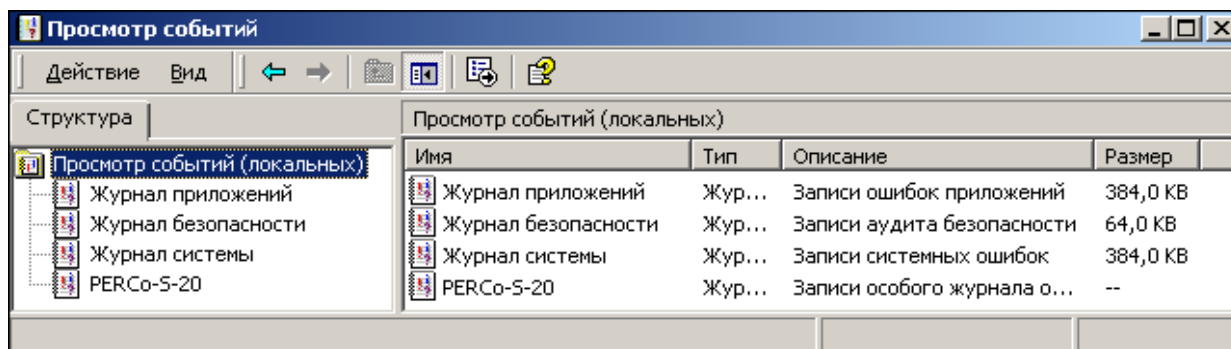
Затем щелкните на [Удалить файл архива \(Del\)](#). В открывшемся диалоговом окне ответьте утвердительно на предупреждение о невозможности последующего восстановления данных.

СООБЩЕНИЯ ОБ ОШИБКАХ

Учитывая, что сервер системы и сервер видеонаблюдения, выполнены в виде стандартных сервисов Windows, информация о возникшей ошибке не может быть выведена в диалоговое окно.

Сообщения об внутренних ошибках, и дополнительная информация записывается в журнал, доступный для просмотра через панель управления Windows.

Для просмотра событий откройте панель управления Windows (**Пуск → Настройка → Панель управления**), далее откройте панель **Администрирование** и запустите **Просмотр событий**.



Информация об ошибках и внутренних сообщения записывается в журнал PERCo-S-20

ПОМЕЩЕНИЯ

Раздел Помещения предназначен для построения схемы помещений школы и устройств. Под помещениями в системе безопасности подразумевается иерархическая структура помещений школы. Эта информация необходима для определения уровней доступа, указания какие контроллеры контролируют доступ в какое помещение, привязки шлейфов охранной сигнализации, видеокамер, дополнительных устройств к помещениям, в которых они установлены.

В данном разделе помещения строятся в виде древовидной структуры. Максимальное количество вложений равно 128. Такое представление структуры помещений наиболее полно отражает реальное расположение помещений школы.

Кроме этого структуру представления помещений можно рассматривать и как схему уровней безопасности. То есть каждый следующий уровень есть не что иное как следующий уровень доступа. Так, например, главный вход школы (холл) находится на первом уровне доступа, переход из этого холла в другие помещения - это уже переход на следующий уровень доступа, соответственно в дереве помещений он отображается как второй уровень вложенности.

РАБОЧЕЕ ОКНО

Рабочее окно раздела имеет следующий вид:

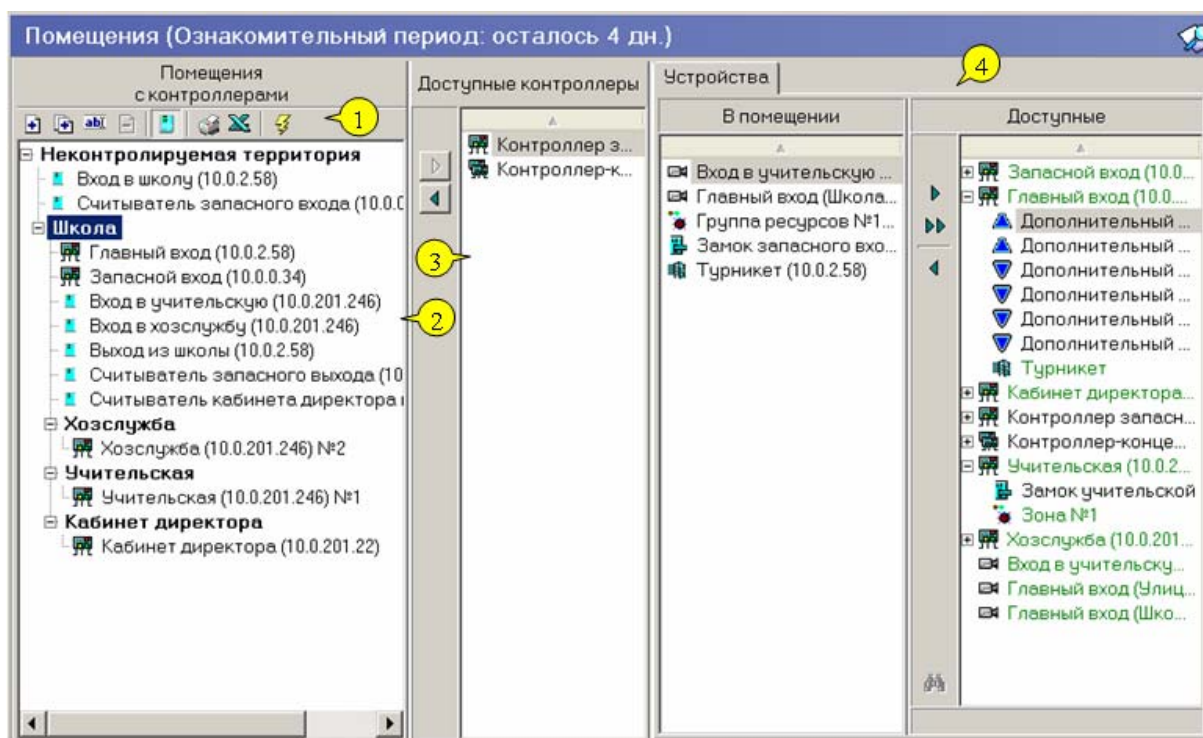


Рис.9. Рабочее окно раздела Помещения

1. Функциональные элементы для работы с помещениями:



1 2 3 4 5 6 7 8

- 1 — Добавить помещение
- 2 — Добавить внутреннее помещение в выделенное помещение
- 3 — Изменить название
- 4 — Удалить помещение
- 5 — Показывать считыватели
- 6 — Печать
- 7 — Экспорт в Excel
- 8 — Передать зоны безопасности считывателей

2. Рабочая область Помещения с контроллерами.

3. Рабочая область Доступные контроллеры.

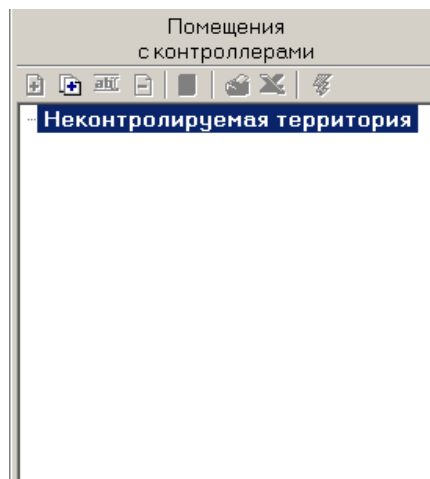
4. Рабочая область Устройства.

ДЕРЕВО ПОМЕЩЕНИЙ

В дереве помещений отображаются контроллеры и, по желанию пользователя, считыватели. С выделением любого из них внизу рабочей области Помещения и

контроллеры открывается информационная панель, сообщающая о помещениях, доступ в которые они обеспечивают.

Список помещений организован в виде дерева, указывающим местоположение помещений. Изначально он пуст, в нем всего лишь один элемент — корень дерева, виртуальное помещение «Неконтролируемая территория»:



Все реальные помещения будут «детьми» этого виртуального помещения.

Таким образом, все помещения, которые будут на один уровень ниже, добавляются как внутренние.

Добавление помещения происходит относительно выделенного в данный момент — или на его уровень или на 1 уровень ниже.

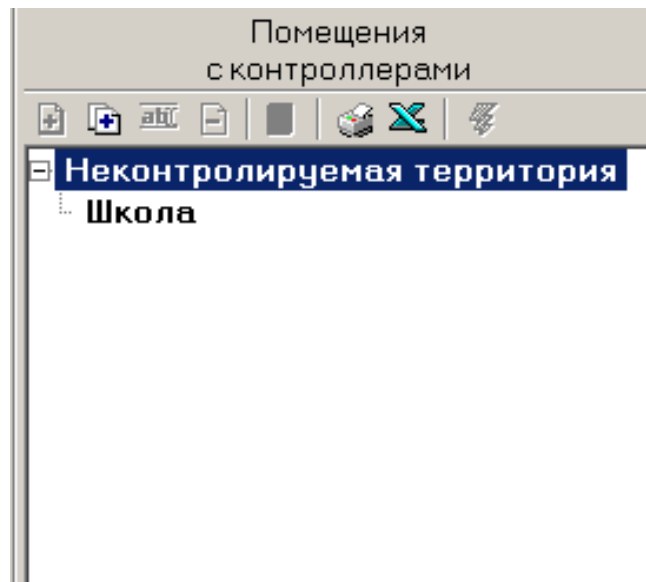
Добавление внутреннего помещения

Для добавления в список внутреннего помещения:

1. Выделите помещение, в которое будет добавлено внутреннее помещение, и щелкните на кнопке **Добавить внутреннее помещение в выделенное помещение** .
2. Откроется окно, в поле которого введите имя нового помещения.



3. Щелкните на кнопке «**ОК**» для отображения нового внутреннего помещения в списке:

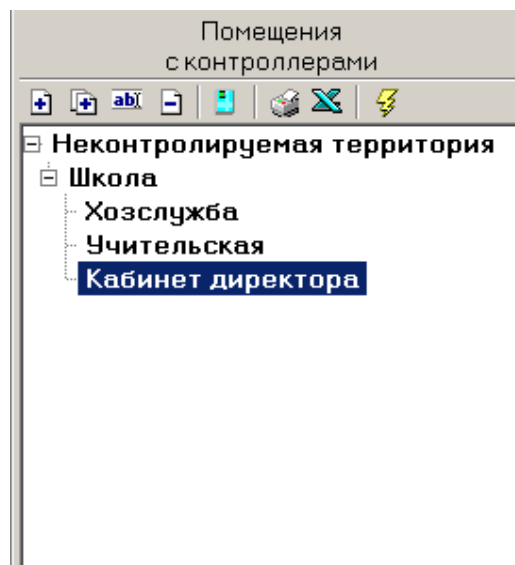


4. Сохраните изменения щелчком на кнопке **Сохранить** — в основном меню Консоли управления.

Добавление помещения на уровень выделенного помещения

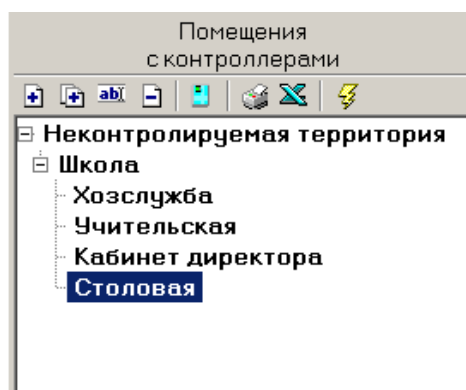
Для добавления в список нового помещения на том же уровне, что и уровень выделенного:

- Выделите помещение.



- Щелкните на кнопке **Добавить помещение** —  . Откроется окно ввода названия нового помещения:

- Введите название помещения.
- Щелкните на кнопке «**OK**» для подтверждения. Новое помещение добавится в список:

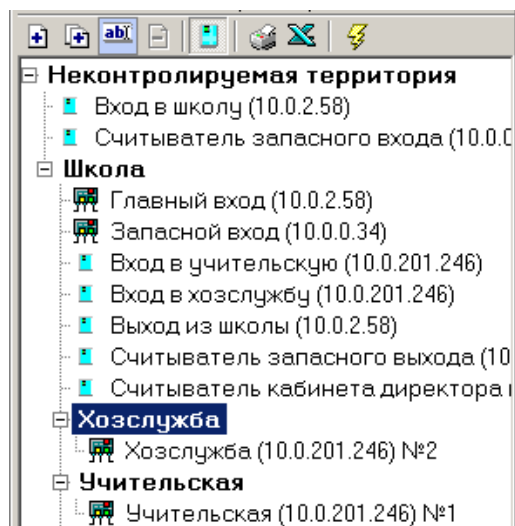


- Сохраните изменения щелчком на кнопке **Сохранить** —  **Сохранить** в основном меню Консоли управления.

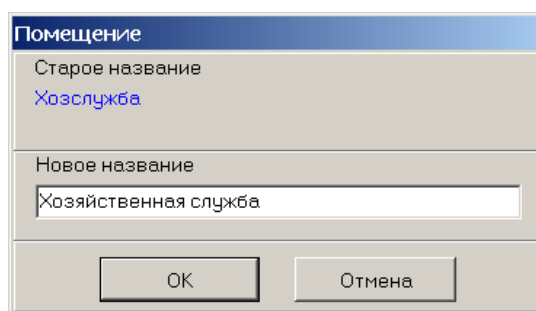
Изменение названия помещения

Для изменения названия помещения:

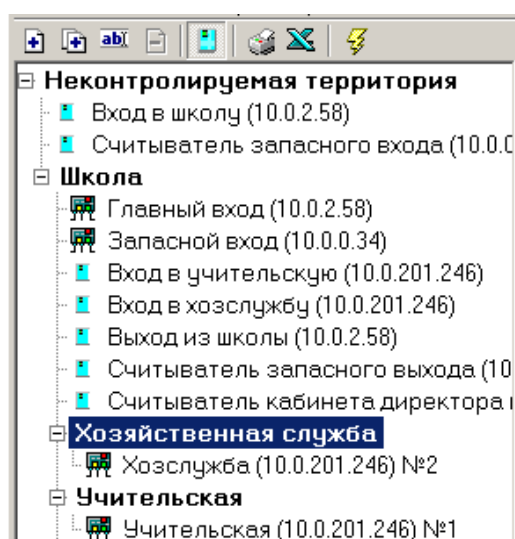
1. Выделите помещение и щелкните на кнопке **Изменить название** —  :



2. Откроется окно ввода и редактирования названия, в поле ввода которого наберите новое название помещения:



3. Подтвердите ввод щелчком на кнопке «ОК». Новое название отобразится в списке:



4. Сохраните изменения щелчком по кнопке **Сохранить** —  **Сохранить** в основном меню Консоли управления.

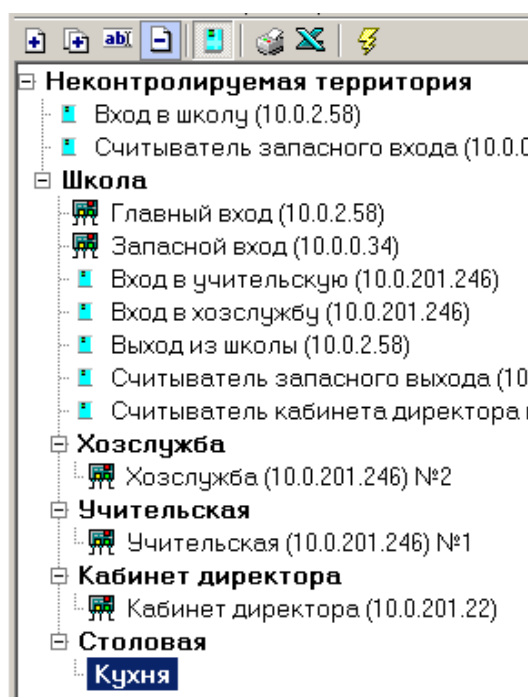
Удаление помещения

Удалить помещение из списка можно только в том случае, если в нем нет ни одного контроллера, за ним не закреплено ни одно устройство и если в нем нет внутренних помещений.

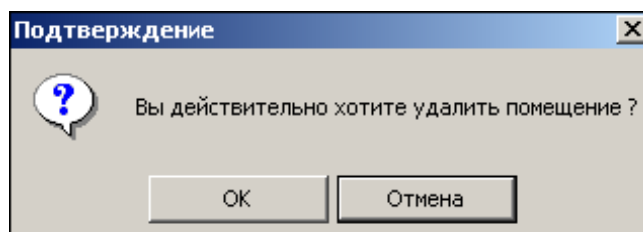
Другими словами, если необходимо удалить помещение из дерева, вы должны сначала удалить из него все связанные с ним устройства системы (см. [«Удаление контроллера из помещения»](#)).

Для удаления помещения:

- Выделите в списке помещение и щелкните на кнопке **Удалить помещение** —  :



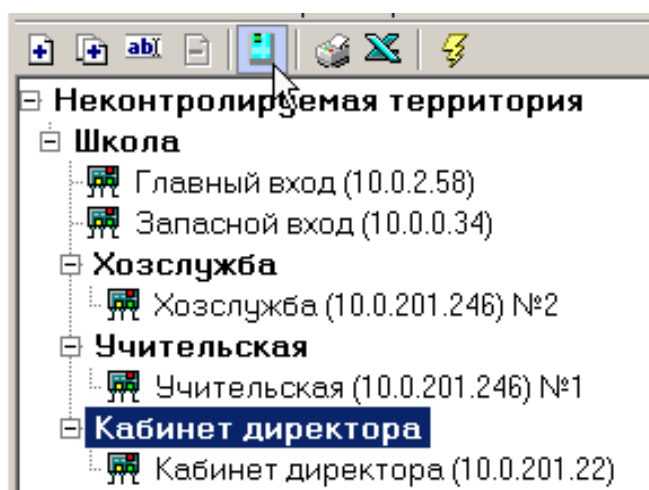
- На экран выводится окно подтверждения:



- Щелкните на кнопке «ОК» для подтверждения удаления выбранного помещения.
- Сохраните изменения щелчком на кнопке **Сохранить** — в основном меню Консоли управления.

Считыватели в дереве помещений

Кнопка **Показывать считыватели**  позволяет увидеть, в каких помещениях расположены считыватели контроллеров:

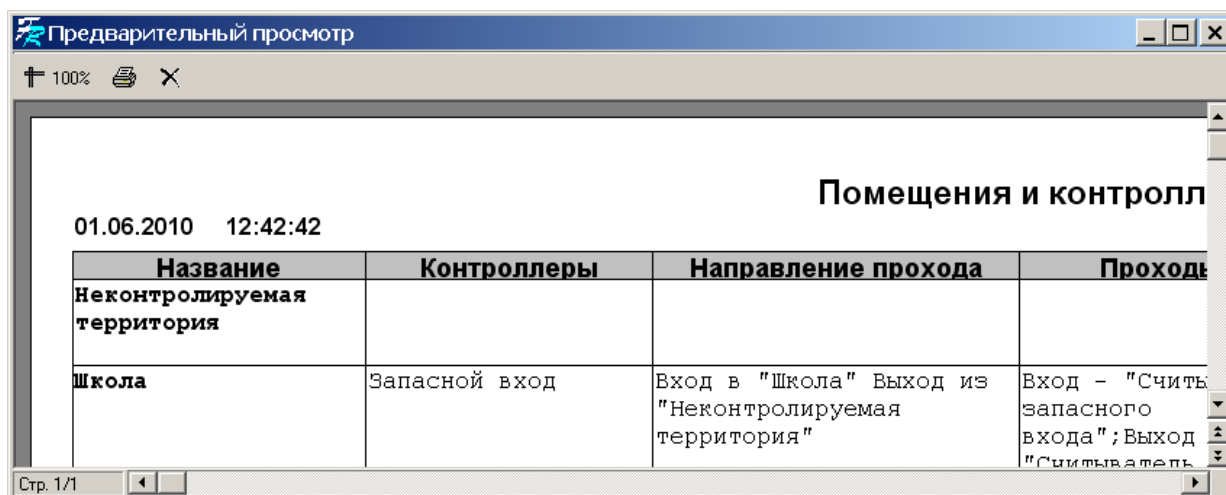


Повторный щелчок по кнопке отменит отображение считывателей.

Печать

Для печати:

1. Щелкните на кнопке **Печать** — . Откроется окно предварительного просмотра:



2. Для вывода таблицы на печать щелкните на кнопке **Печать отчёта** — .

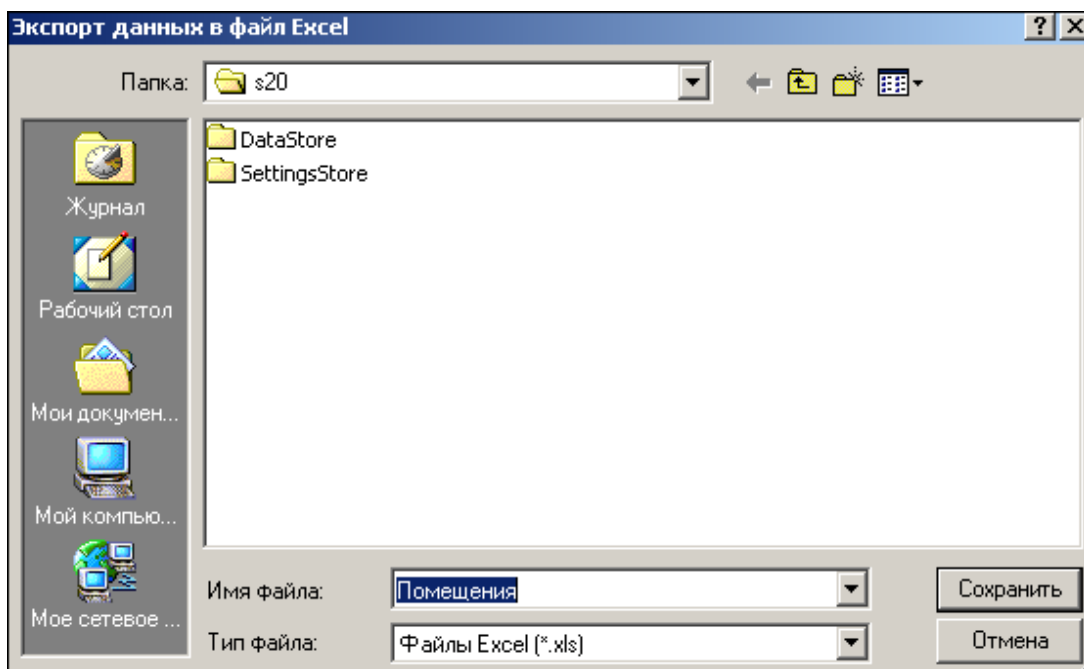
Масштаб —  100% для настройки масштаба отображения отчёта.

Выход —  для закрытия предварительного просмотра документа.

Экспорт в Excel

Для экспорта данных о подразделениях в файл формата Microsoft Excel:

1. Щелкните на кнопке **Экспорт в Excel** — . На экране откроется стандартное окно **Экспорт данных в Excel**:



2. Выберите диск и папку, введите имя файла и щелкните на кнопке **Сохранить**. Данные будут сохранены в указанном файле.

Изменение структуры дерева помещений

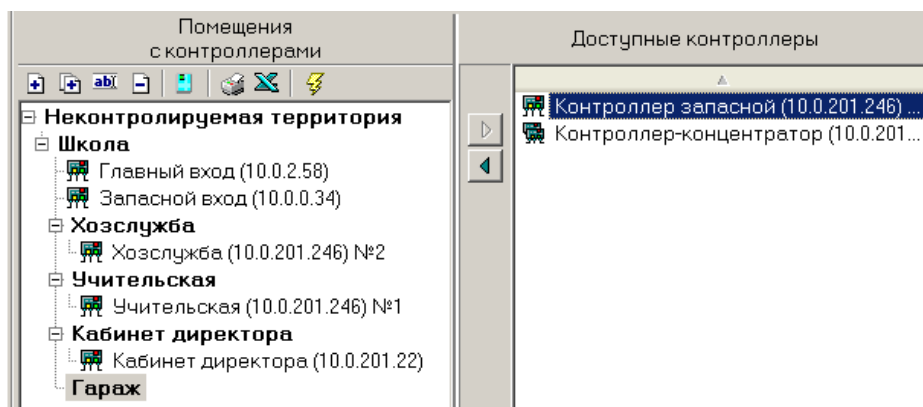
Система позволяет изменить структуру дерева помещений - с помощью стандартной в Windows операции Drag/Drop.

1. Чтобы помещение стало внутренним для другого помещения, захватите мышкой перемещаемое помещение и, не отжимая кнопку мышки, переместите мышку на название того помещения, которое станет "родителем" перемещаемого помещения.
2. Чтобы нужное помещение "встало" перед другим помещением (на уровне этого помещения), захватите нужное помещение мышкой и, не отжимая кнопку мышки, переместите мышку на место слева от названия другого помещения.

ДОСТУПНЫЕ КОНТРОЛЛЕРЫ

Как уже описывалось выше, основной целью создания дерева помещений является создание структуры распределения контроллеров системы безопасности по территории школы и определение уровней безопасности (доступа). Для этого после создания самого дерева помещений необходимо перейти к территориальной привязке устройств системы безопасности.

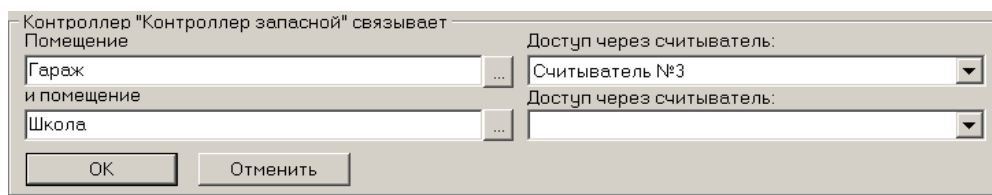
Осуществляя привязку контроллеров доступа к помещениям предприятия (организации), Вы тем самым указываете, какой именно контроллер управления доступом будет контролировать вход в это помещение и из какого помещения осуществляется этот вход. Указание помещения, из которого осуществляется вход в выбранное помещение обусловлено тем, что структура дерева не всегда может точно отражать многообразие архитектурных решений и уровней безопасности. В действительности помещение, расположенное в самой глубине предприятия, может иметь пожарный выход, позволяющий выйти за пределы контролируемой территории. Рабочая область **Доступные контроллеры** содержит в себе список контроллеров, которые готовы к работе:



Для добавления контроллера в помещение:

1. Укажите помещение, в которое будет определен контроллер.
2. Выделите щелчком мыши нужный контроллер из списка доступных контроллеров.
3. Щелкните на кнопке **Добавить контроллер в помещение** —  .

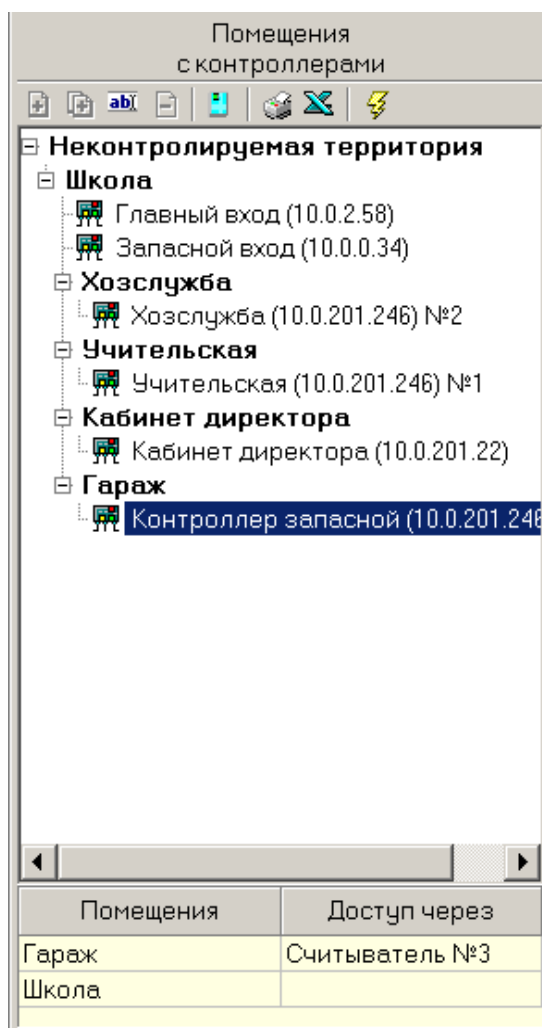
После этого в нижней части рабочего окна появится панель ввода и редактирования данных о помещениях, которые связывает новый контроллер, и направлениях проходов:



Значение можно выбрать из дополнительного окна выбора щелчком на кнопке, или комбинированного списка щелчком на кнопке .

Доступ через считыватель позволяет выбрать считыватель из списка считывателей добавляемого контроллера, который будет контролировать проход в помещение указанное слева от считывателя.

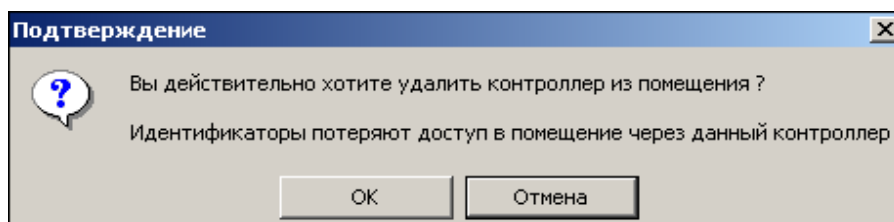
4. После заполнения подтвердите ввод щелчком на кнопке «**ОК**». Добавленный контроллер отобразится в дереве помещений. Из списка доступных контроллеров он удалится:



5. Передайте измененные данные в аппаратуру с помощью кнопки **Передать зоны безопасности считывателей** .

Для удаления контроллера из помещения:

1. Выделите контроллер, который подлежит удалению.
2. Щелкните на кнопке **Удалить контроллер из помещения** — . Откроется окно подтверждения:



После подтверждения контроллер переместится из списка помещений в список доступных контроллеров.

УСТРОЙСТВА

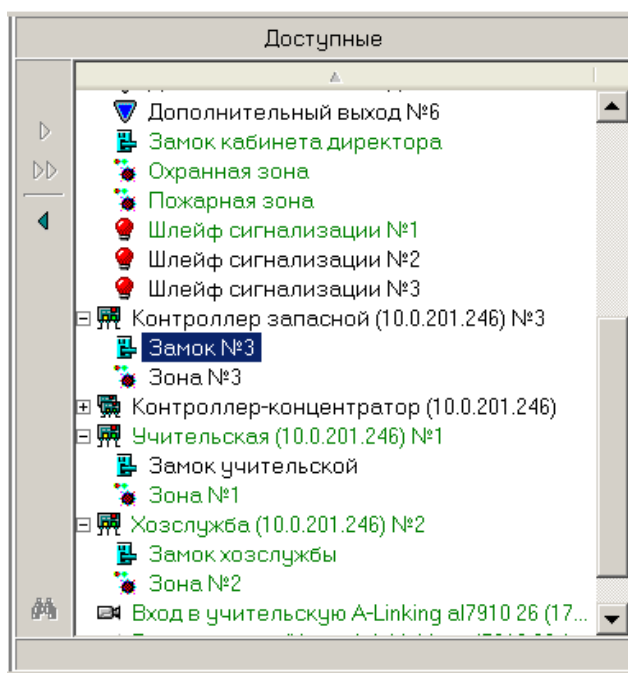
Кроме контроллеров управления доступом, привязка которых к помещениям обусловлена определением того, какой контроллер контролирует доступ в то или иное помещение, можно привязать к помещениям и остальные устройства системы. Благодаря этому система, во-первых, сможет однозначно указывать места происхождений событий в системе. Во-вторых, это позволит выполнять команды на помещении: такие команды будут выполнены для всех однотипных устройств конкретного помещения.

Рабочая область **Устройства** разделена на два списка : **В помещении** и **Доступные**.

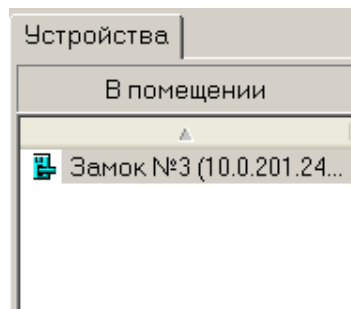
В списке **Доступные** - все доступные для использования устройства.

Для **добавления устройства** в помещение:

1. В списке **Доступные** выделите устройство, которое будет закреплено за выделенным в данный момент помещением:

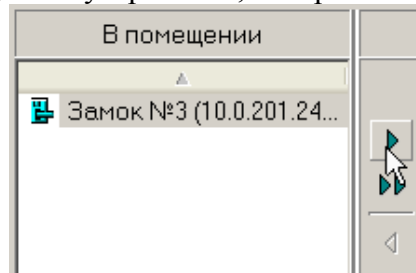


2. Щелкните на кнопке **Закрепить устройство за помещением** — . Устройство скопируется в окно **В помещении**.



Для **удаления устройства** из помещения:

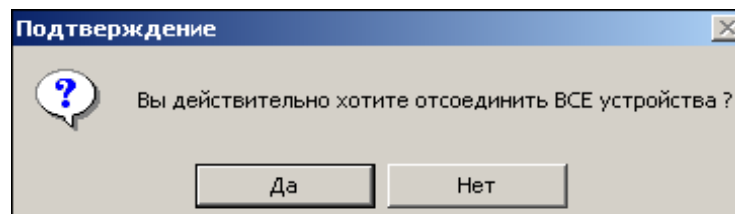
1. В списке **В помещении** выделите устройство, которое необходимо удалить.



2. Щелкните на кнопке **Удалить устройство из помещения** — . Устройство переместится в список **Доступные**.

Для **удаления одновременно всех устройств**

1. Щелкните на кнопке **Удалить все устройства** — . Откроется окно подтверждения::



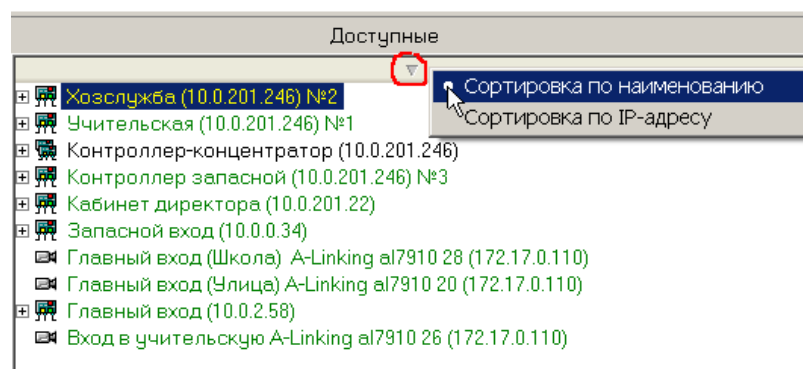
2. Щелкните на кнопке «**Да**» для подтверждения.

В списке доступных устройств зеленым цветом выделяются устройства, уже закрепленные за помещением (помещениями). Название этого помещения - под списком.

С помощью кнопки , расположенной внизу и слева от списка, в дереве помещений выделяется помещение, за которым закреплено выделенное в данный момент устройство.

СОРТИРОВКА СПИСКОВ

Способ сортировки списков доступных контроллеров, устройств в помещении, доступных устройств определяется с помощью контекстного меню, отображающегося по клику правой кнопкой мыши на заголовке соответствующего списка.



Щелчком мыши на кнопку сортировки устройства сортируются в прямом () и обратном алфавитном порядке () или по нарастанию () и убыванию IP-адреса () в зависимости от выбора критерия сортировки.

ТРЕБОВАНИЯ К АППАРАТУРЕ

Компьютеры:

Объем дискового пространства:

Сервер системы: 100 Гб.

Сервер видеонаблюдения: Для хранения видеоизображения не менее 300 Гб.

Станция: 1 Гб.

Оперативная память:

Сервер системы: 3 Гб.

Сервер видеонаблюдения: 3 Гб.

Станция: 2 Гб.

Процессор:

Сервер системы: не ниже Pentium 4

Сервер видеонаблюдения: не ниже Pentium 4

Станция: не ниже Celeron 2.5

Операционная система: Windows 2000 Prof., Windows 2003.

Для станции Windows XP, Windows 2000 Prof., Windows 2003.

Для сервера системы и сервера видеонаблюдения допустимо использование 64 битных версий операционных систем.

Сеть: 100 Mbit.

Рекомендуемые GSM USB-модемы - HUAWEI от операторов Мегафон и МТС и ONEXT USB GSM modem.

Камеры и видеосервера:

ПРИЛОЖЕНИЕ 1. СОБЫТИЯ

СОБЫТИЯ, ЗАПИСЫВАЕМЫЕ В ЖУРНАЛ РЕГИСТРАЦИИ

События контроллера доступа (серия CL01, CL02, CL03, CT01, KT02)

События, связанные с перемещением через ИУ

Запрет прохода с причиной:

- *идентификатор НЕ ЗАРЕГИСТРИРОВАН* – предъявленный идентификатор никогда не передавался в контроллер, то есть ему не назначались права доступа в этот контроллер;
- *идентификатор ЗАПРЕЩЁН* - доступ предъявленному идентификатора явным образом запрещен в контроллере, то есть данный контроллер включен в список доступа предъявленного идентификатора с явным запрещением проходов;
- *идентификатор из СТОП-ЛИСТА* - предъявленный идентификатор занесен в «СТОП-ЛИСТ»;
- *идентификатор ПРОСРОЧЕН* — у предъявленного идентификатора истек срок действия, указанный в параметрах доступа;
- *нарушение ВРЕМЕНИ* - у данного контроллера установлен «жесткий» контроль времени, а предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* - у данного контроллера установлена «жесткая» защита от передачи идентификаторов, а предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* - это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение ЗОНАЛЬНОСТИ*;
- *нарушение КОМИССИОНИРОВАНИЯ* - было зафиксировано несоответствие с комиссионировавшим идентификатором или комиссионирование не было выполнено вообще;
- *запрет по команде от ДУ* - охранник пультом ДУ подал команду на запрет прохода, после того, как контроллер разрешил проход;
- *запрет по команде от ПО* - оператор с ПК подал команду на запрет прохода, после того, как контроллер разрешил проход;
- *отказ в подтверждении от ВЕРИФИКАЦИИ* - не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *нарушение РЕЖИМОВ РАБОТЫ* – у данного контроллера установлен такой режим работы, при котором доступ по предъявленному идентификатору запрещен (режимы «ЗАКРЫТО» и «ОХРАНА»);

Отказ от прохода - отказ от предоставленного системой права пройти через ИУ по идентификатору.

Проход — событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером права пройти через него и до истечения времени удержания ИУ в открытом состоянии, без каких-либо выявленных нарушений.

Проход с причиной нарушения:

- *нарушение ВРЕМЕНИ* – у данного контроллера установлен «мягкий» контроль времени, а предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* – у данного контроллера установлена «мягкая» защита от передачи идентификаторов, а предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение ЗОНАЛЬНОСТИ*;
- *нарушение КОМИССИОНИРОВАНИЯ* – было зафиксировано несоответствие с комиссионирующим идентификатором или комиссионирование не было выполнено вообще;
- *нарушение ВРЕМЕНИ и КОМИССИОНИРОВАНИЯ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение КОМИССИОНИРОВАНИЯ*;
- *нарушение ЗОНАЛЬНОСТИ и КОМИССИОНИРОВАНИЯ* – это комбинация двух причин, описанных выше: *нарушение ЗОНАЛЬНОСТИ* и *нарушение КОМИССИОНИРОВАНИЯ*;
- *нарушение ВРЕМЕНИ, ЗОНАЛЬНОСТИ и КОМИССИОНИРОВАНИЯ* – это комбинация трех причин, описанных выше: *нарушение ВРЕМЕНИ*, *нарушение ЗОНАЛЬНОСТИ* и *нарушение КОМИССИОНИРОВАНИЯ* ;
- *нарушение ВЕРИФИКАЦИИ* – в результате верификации предъявленного идентификатора, контроллером не было получено подтверждения от верифицирующего устройства в данном направлении, но проход был осуществлен в другом направлении и по другому считывателю;
- *нарушение ВРЕМЕНИ и ВЕРИФИКАЦИИ* - в результате верификации предъявленного идентификатора, контроллером не было получено подтверждения от верифицирующего устройства в данном направлении, но проход был осуществлен с *нарушением ВРЕМЕНИ* в другом направлении и по другому считывателю;
- *нарушение ЗОНАЛЬНОСТИ и ВЕРИФИКАЦИИ* - в результате верификации предъявленного идентификатора, контроллером не было получено подтверждения от верифицирующего устройства в данном направлении, но проход был осуществлен с *нарушением ЗОНАЛЬНОСТИ* в другом направлении и по другому считывателю;
- *нарушение ВРЕМЕНИ, ЗОНАЛЬНОСТИ и ВЕРИФИКАЦИИ* - это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ и ВЕРИФИКАЦИИ* и *нарушение ЗОНАЛЬНОСТИ и ВЕРИФИКАЦИИ*;

Проход, подтверждение от ДУ – событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером с подтверждением от ДУ права прохода и до истечения времени удержания ИУ в открытом состоянии. Подтверждение от ДУ осуществляется при условии, что стоят опции «подтверждения от ДУ» для верификации сотрудников на каждый считыватель:

- при проходе
- при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ.

Проход с подтверждением от ДУ и причиной нарушения:

- нарушение ЗОНАЛЬНОСТИ – предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода.

Проход, подтверждение от ВЕРИФИКАЦИИ - событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером с подтверждением от верифицирующего устройства права прохода и до истечения времени удержания ИУ в открытом состоянии. Подтверждение от верифицирующего устройства осуществляется в соответствии с параметрами, задаваемыми в разделе «ВЕРИФИКАЦИЯ» для верификации сотрудников на каждый считыватель:

- при проходе;
- при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ ;

Проход с подтверждением от ВЕРИФИКАЦИИ и причиной нарушения:

- нарушение ЗОНАЛЬНОСТИ – предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;

ИУ не закрыто после прохода (с фиксацией номера идентификатора). Событие возникает, если после прохода по идентификатору время активизации состояния контакта ИУ превысило установленное предельное время разблокировки. То есть, например, после открытия дверь остается в открытом состоянии в течение времени большем, чем время удержания в открытом состоянии, установленное для данного контроллера.

Проход по команде от ДУ. Событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером по команде от ДУ права прохода и до истечения времени удержания ИУ в открытом состоянии.

Проход по команде от ПК. Событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером по команде от ПК права прохода и до истечения времени удержания ИУ в открытом состоянии.

Проход по команде от ИК - пульта. Событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером по команде от ИК - пульта права прохода и до истечения времени удержания ИУ в открытом состоянии.

Несанкционированный проход через ИУ (взлом ИУ). Событие, возникающее при активизации состояния контакта ИУ, не сопровождающегося санкционированным системой открытием ИУ. Механической разблокировки двери, турникета с последующим проходом через него.

События, связанные с изменением текущего состояния дополнительных входов

Активизация входа - вызывается срабатыванием устройства, подключенного к данному дополнительному входу.

Нормализация входа — вызывается отключением устройства (переходом в нормальное состояние), подключенного к данному дополнительному входу.

События, связанные с изменением текущего состояния дополнительных выходов

Активизация выхода. Событие происходит в случае подачи контроллером управляющего сигнала на дополнительный выход. Причиной может служить команда от программного обеспечения или выполнение заданной на этапе конфигурации логики работы контроллера.

Нормализация выхода. Событие происходит в случае снятия контроллером управляющего сигнала с дополнительного выхода. Причиной может служить команда от программного обеспечения или выполнение заданной на этапе конфигурации логики работы контроллера.

События, связанные с изменением текущего состояния корпуса контроллера

Корпус контроллера открыт. Событие происходит в случае вскрытия корпуса контроллера.

Корпус контроллера закрыт. Событие происходит при закрытии корпуса контроллера.

События, связанные с работоспособностью сетевых каналов контроллера

Система безопасности взаимодействует с любым контроллером по 3 сетевым каналам. Для нормальной работы контроллера требуется, чтобы все 3 сетевых канала были открыты:

- канал управления — служит для передачи команд управления от системы безопасности к контроллеру. С данным каналом связаны следующие события:
 - *Канал управления ОТКРЫТ* — событие возникает при открытии канала управления сервером системы;
 - *Канал управления ЗАКРЫТ* — событие возникает при закрытии канала управления сервером системы;
 - *Канал управления НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала управления сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу управления другим программным обеспечением (например, локальным ПО);
 - *Канал управления неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом управления контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;

- *Канал управления НЕ АВТОРИЗИРОВАН* — событие возникает при невозможности сервера системы получить авторизованный доступ к контроллеру. Причиной, вызывающей такое событие, является наличие установленного пароля в контроллере, отличного от передаваемого пароля на этот контроллер системой безопасности;
- *Ожидание открытия канала управления*- событие возникает при постановке в очередь сервера системы запроса на открытие канала управления;
- *Отмена ожидания открытия канала управления*- событие возникает при удалении из очереди сервера системы запроса на открытие канала управления;
- *Попытка открытия канала управления* — событие уведомляет о начале операции по открытию канала управления сервером системы;
- *Нарушение связи с каналом управления* — событие возникает при отсутствии связи между сервером системы и каналом управления контроллера в течении 2 мин.;
- *Нет ответа на выполнение команды по каналу управления* — событие возникает в случае отсутствия ответа от контроллера в течении 6 мин. на выполнение команды сервером системы;
- канал мониторинга — служит для получения системой безопасности журнала мониторинга контроллера. С данным каналом связаны следующие события:
- *Канал мониторинга ОТКРЫТ* — событие возникает при открытии канала мониторинга сервером системы;
- *Канал мониторинга ЗАКРЫТ* — событие возникает при закрытии канала мониторинга сервером системы;
- *Канал мониторинга НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала мониторинга сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу мониторинга другим программным обеспечением (например, локальным ПО);
- *Канал мониторинга неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом мониторинга контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;
- *Попытка открытия канала мониторинга* — событие уведомляет о начале операции по открытию канала мониторинга сервером системы;
- *Нарушение связи с каналом мониторинга* — событие возникает при отсутствии связи между сервером системы и каналом мониторинга контроллера в течении 2 мин.;
- канал регистрации - служит для получения системой безопасности журнала регистрации контроллера. С данным каналом связаны следующие события:
- *Канал регистрации ОТКРЫТ* — событие возникает при открытии канала регистрации сервером системы;
- *Канал регистрации ЗАКРЫТ* — событие возникает при закрытии канала регистрации сервером системы;

- *Канал регистрации НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала регистрации сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу регистрации другим программным обеспечением (например, локальным ПО);
- *Канал регистрации неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом регистрации контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;
- *Попытка открытия канала регистрации* — событие уведомляет о начале операции по открытию канала регистрации сервером системы;
- *Нарушение связи с каналом регистрации* — событие возникает при отсутствии связи между сервером системы и каналом регистрации контроллера в течении 2 мин.;

События, связанные с изменением текущего состояния контроллеров или системы

Включение или выключение питания контроллера. Выключение питания может возникнуть в двух случаях: или при штатном выключении блока питания контроллера, или при аварийном выключении, связанным с аварией сети и разрядом аккумулятора. Включение питания возникает аналогично выключению в двух случаях: или при штатном включении блока питания контроллера, или при восстановлении сетевого питания.

Нарушение или восстановление связи с контроллером. Эти события относятся к разряду диагностических и отражают возможное нарушение и восстановление работоспособности структурных элементов системы. Такие события возникают при нарушении связи между программным обеспечением системы безопасности и контроллером. Через 2 минуты отсутствия связи по одному из каналов контроллера, соединение по всем каналам будет закрыто. События генерируется при нарушении связи с

- каналом управления;
- каналом мониторинга;
- каналом регистрации;

Переполнение или очистка журнала регистрации. Переполнение журнала возникает после заполнения в памяти контроллера свободной предпоследней страницы журнала (размер одной страницы равен 32 событиям). Очистка журнала происходит всегда после чтения переполненного журнала регистрации.

Переполнение списка идентификаторов. Событие появляется в случае, если из-за внутренней ошибки программного обеспечения в контроллер передано количество карт доступа, превышающее его ресурсы.

Ошибка принятого сообщения. Событие возникает в случае невозможности контроллера правильно декодировать принятые от программного обеспечения сообщения. Может быть вызвано ошибками сети Ethernet.

Перезапуск контроллера. Событие возникает в случае решения контроллера о поведении аппаратного сброса. Данные события носят диагностический характер:

- *внешний сброс;*
- *сброс по WatchDog.*

Неисправность контроллера. Приведенные ниже события носят диагностический характер и содержат информацию о выходе из строя составляющих контроллера:

- *памяти FRAM;*
- *памяти DataFlash;*
- *памяти SRAM;*
- *часов RTC;*
- *шины I²C.*

Форматирование памяти событий. Приведенные ниже события содержат информацию об изменении состояния внутренней памяти контроллера и носят диагностический характер:

- *область журнала событий;*
- *область списка карт;*
- *область установок конфигурации;*
- *область программ;*
- *область текущих установок.*

Изменение режима работы (PP) по команде от ПО. Событие регистрируется контроллером при изменении режима работы оператором из программного обеспечения.

Изменение PP на/с PP «Охрана». Событие возникает при постановке/снятии с охраны группы ресурсов, в которую входит ИУ. Выход из PP «Охрана» производится в PP «Контроль».

Изменение PP по команде от ИК. Событие регистрируется при смене режима контроля доступа в результате команды получаемой контроллером управления доступом от ИК пульта управления.

Тревога по команде от ИК-пульта. Событие регистрируется при получении команды поднятия тревоги от ИК пульта управления..

Авария или восстановление питания. Авария возникает в случае понижения напряжения питания контроллера ниже уровня 10 вольт. Восстановление происходит в случае установления нормального уровня напряжения - 12 вольт.

Тревога или сброс тревоги по команде от ПО. События связаны с возникновением тревожной ситуации в системе (см. параметры генератора тревоги) и сбросом сигнала тревоги оператором системы под управлением ПО "Управление системой" или активизацией дополнительного входа сброса тревоги.

Тревога по вскрытию корпуса извещателя. Событие происходит в случае вскрытия корпуса извещателя, подключенного к шлейфам ОПС, при условии, что извещатель имеет датчик вскрытия корпуса.

Корпус извещателя закрыт. Событие возникает при закрытии предварительно открытого корпуса извещателя, подключенного к шлейфам ОПС, при условии, что извещатель имеет датчик вскрытия корпуса.

События, связанные с изменениями состояний группы ресурсов

ГР взята на охрану по идентификатору. Событие возникает при взятии на охрану всей группы ресурсов по идентификатору с соответствующими правами. Если группа ресурсов включает в себя ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Охрана».

ГР снята с охраны по идентификатору. Событие возникает при снятии с охраны группы ресурсов по идентификатору с соответствующими правами. Если группа ресурсов включает в себя ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Контроль».

Попытка взятия ГР на охрану (невозможно взять) по идентификатору. Событие возникает при попытке взятия на охрану по идентификатору группы ресурсов:

- *нарушение состояния дополнительного входа.* Событие возникает, если в процессе постановки группы ресурсов на охрану состояние дополнительного входа было не нормализовано. Например, датчик движения, подключенный к данному дополнительному входу, находится в активном состоянии;
- *нарушение состояния ресурса ИУ.* Событие возникает, если в процессе постановки группы ресурсов на охрану состояние ресурса ИУ было не нормализовано. Например, это может происходить при постановке на охрану при открытой двери;
- *нарушение КОМИССИОНИРОВАНИЯ.* Событие возникает, если в процессе постановки группы ресурсов на охрану было зафиксировано несоответствие с комиссионировающим идентификатором или комиссионирование не было выполнено вообще;
- *нарушение ВЕРИФИКАЦИИ.* Событие возникает, если в процессе постановки группы ресурсов на охрану не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *нарушение ВРЕМЕНИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану группы ресурсов без ИУ и являющегося нарушителем по времени;
- *нарушение ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану группы ресурсов и являющегося нарушителем зональности;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану группы ресурсов и являющуюся нарушителем и по времени и зональности;
- *отказ от постановки.* Событие возникает, если после поднесения к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану группы ресурсов и до истечения времени удержания ИУ в открытом состоянии, этот идентификатор не был поднесен повторно.

Попытка снятия ГР с охраны (невозможно снять) по идентификатору. Событие возникает при попытке снятия с охраны по идентификатору группы ресурсов:

- *нарушение КОМИССИОНИРОВАНИЯ.* Событие возникает, если в процессе снятия группы ресурсов с охраны было зафиксировано несоответствие с комиссионировающим идентификатором или комиссионирование не было выполнено вообще;

- *нарушение ВЕРИФИКАЦИИ.* Событие возникает, если в процессе снятия группы ресурсов с охраны не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *нарушение ВРЕМЕНИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны любой группы ресурсов и являющегося нарушителем по времени;
- *нарушение ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны любой группы ресурсов и являющегося нарушителем зональности;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны любой группы ресурсов и являющегося нарушителем и по времени и по зональности;
- *отказ от снятия.* Событие возникает, если после поднесения к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны любой группы ресурсов и до истечения времени удержания ИУ в открытом состоянии этот идентификатор не был поднесен повторно.

Невзятие ГР на охрану по идентификатору. Событие возникает, если после попытки взятия группы ресурсов на охрану по идентификатору один или несколько из входящих в нее ресурсов окажется в состоянии «невзятие».

ГР взята на охрану по идентификатору, подтверждение от ВЕРИФИКАЦИИ. Событие возникает при взятии на охрану всех ресурсов группы ресурсов по идентификатору с соответствующими правами и с подтверждением от верифицирующего устройства. Если группа ресурсов включает в себя ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Охрана».

ГР снята с охраны по идентификатору, подтверждение от ВЕРИФИКАЦИИ. Событие возникает при снятии с охраны группы ресурсов по идентификатору с соответствующими правами и с подтверждением от верифицирующего устройства. Если группа ресурсов включает в себя ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Контроль».

ГР взята на охрану по команде от ПО. Событие возникает при взятии на охрану всей группы ресурсов по команде оператора ПК. Если группа ресурсов включает в себя ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Охрана».

ГР снята с охраны по команде от ПО. Событие возникает при снятии с охраны группы ресурсов по команде оператора ПК. Если группа ресурсов включает в себя ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Контроль».

Попытка взятия ГР на охрану (невозможно взять) по команде от ПО. Событие возникает при попытке взятия на охрану по команде оператора ПК группы ресурсов:

- *нарушение состояния дополнительного входа.* Событие возникает, если в процессе постановки группы ресурсов на охрану состояние данного дополнительного входа было не нормализовано;
- *нарушение состояния ИУ.* Событие возникает, если в процессе постановки группы ресурсов на охрану состояние ресурса ИУ было не нормализовано.

Невзятие ГР на охрану по команде от ПО. Событие возникает, если после попытки взятия группы ресурсов на охрану по команде оператора ПК один или несколько из входящих в нее ресурсов окажутся в состоянии «невзятие».

Тихая тревога по ГР. Событие возникает, если один или несколько ресурсов, входящих в группу ресурсов, перейдут в состояние «Тихая тревога».

Тревога по ГР. Событие возникает, если один или несколько ресурсов, входящих в группу ресурсов, перейдут в состояние «Тревога».

Сброс тревоги по ГР по команде от ПО. Событие возникает, при начале процедуры сброса тревоги всей группы ресурсов по команде оператора от ПК.

Взятие ГР на охрану по идентификатору. Событие возникает при начале процедуры взятия на охрану всей группы ресурсов по идентификатору с соответствующими правами (идет задержка взятия).

Взятие группы ресурсов на охрану по команде оператора. Событие возникает при начале процедуры взятия на охрану всей группы ресурсов по команде оператора (идет задержка взятия).

События, связанные с изменением текущего состояния ресурсов, входящих в группу ресурсов

Невзятие на охрану ресурса "Шлейф сигнализации". Событие возникает, если в момент взятия группы ресурсов на охрану состояние входящего в нее ШС окажется не нормализованным. ШС перейдет в состояние «невзятие».

Взят на охрану ресурс. Событие возникает при переходе ресурса в состояние «взят» с указанием типа ресурса:

- ресурс "Дополнительный вход";
- ресурс "ИУ";
- ресурс "Шлейф сигнализации".

Взятие на охрану ресурса. Событие возникает в момент взятия группы ресурсов на охрану: для ИУ – всегда, для ШС - если установлено не нулевое значение параметра «Задержка взятия на Охрану»:

- ресурс "ИУ";
- ресурс "Шлейф сигнализации".

Снят с охраны ресурс. Событие возникает при переходе ресурса в состояние «снят» с указанием типа ресурса:

- ресурс "Дополнительный вход";
- ресурс "ИУ";
- ресурс "Шлейф сигнализации".

Неисправность снятого ресурса "Шлейф сигнализации". Событие возникает, если величина сопротивления ШС, у которого параметр «задержка восстановления нарушенного ШС в снятом состоянии» отличен от значений 0 либо 255, и не

находящегося в режиме «Охрана», не находится в пределах от 2 до 10 кОм, либо изменилось более чем на 10% в течение часа.

Нормализация снятого ресурса "Шлейф сигнализации". Событие возникает при нормализации состояния ШС, находившегося в состоянии «неисправность снятого ШС».

Нарушение ресурса, состояние «Тревога». Событие возникает при переходе ресурса в состояние «Тревога»:

- ресурс "Дополнительный вход"
- ресурс "ИУ"
- ресурс "Шлейф сигнализации"

Нарушение ресурса, состояние «Тихая тревога». Событие возникает при переходе ресурса в состояние «Тихая тревога»:

- ресурс "Шлейф сигнализации"

Восстановление ресурса. Событие возникает при нормализации состояния ресурса, находящегося в состоянии «Тревога» с указанием типа ресурса:

- ресурс "Шлейф сигнализации"

Сброс тревоги ресурса. Событие возникает при сбросе тревоги по ресурсу:

- ресурс "Дополнительный вход"
- ресурс "ИУ";
- ресурс "Шлейф сигнализации"

Автономный сброс сирены. Событие возникает при сбросе сирены по входу автономного сброса сирены.

События контроллеров КБО (серия CS01)

События, связанные с перемещением через ИУ

Запрет прохода с причиной:

- *идентификатор НЕ ЗАРЕГИСТРИРОВАН* — предъявленный идентификатор никогда не передавался в контроллер, то есть ему не назначались права доступа в этот контроллер;
- *идентификатор ЗАПРЕЩЁН* - доступ предъявленному идентификатору явным образом запрещен в контроллере, то есть данный контроллер включен в список доступа предъявленного идентификатора с явным запрещением проходов;
- *идентификатор из СТОП-ЛИСТА* - предъявленный идентификатор занесен в «СТОП-ЛИСТ»;
- *идентификатор ПРОСРОЧЕН* — у предъявленного идентификатора истек срок действия, указанный в параметрах доступа;

- *нарушение ВРЕМЕНИ* - у данного контроллера установлен «жесткий» контроль времени, а предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* - у данного контроллера установлена «жесткая» защита от передачи идентификаторов, а предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* - это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение ЗОНАЛЬНОСТИ*;
- *нарушение КОМИССИОНИРОВАНИЯ* - было зафиксировано несоответствие с комиссионировающим идентификатором или комиссионирование не было выполнено вообще;
- *запрет по команде от ДУ* - охранник пультом ДУ подал команду на запрет прохода, после того, как контроллер разрешил проход;
- *запрет по команде от ПО* - оператор с ПК подал команду на запрет прохода, после того, как контроллер разрешил проход;
- *отказ в подтверждении от ВЕРИФИКАЦИИ* - не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *нарушение РЕЖИМОВ РАБОТЫ* – у данного контроллера установлен такой режим работы, при котором доступ по предъявленному идентификатору запрещен (режимы «ЗАКРЫТО» и «ОХРАНА»);

Отказ от прохода - отказ от предоставленного системой права пройти через ИУ по идентификатору.

Проход — событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером права пройти через него и до истечения времени удержания ИУ в открытом состоянии, без каких-либо выявленных нарушений.

Проход с причиной нарушения:

- *нарушение ВРЕМЕНИ* – у данного контроллера установлен «мягкий» контроль времени, а предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* – у данного контроллера установлена «мягкая» защита от передачи идентификаторов, а предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение ЗОНАЛЬНОСТИ*;
- *нарушение КОМИССИОНИРОВАНИЯ* – было зафиксировано несоответствие с комиссионировающим идентификатором или комиссионирование не было выполнено вообще;
- *нарушение ВРЕМЕНИ и КОМИССИОНИРОВАНИЯ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение КОМИССИОНИРОВАНИЯ*;
- *нарушение ЗОНАЛЬНОСТИ и КОМИССИОНИРОВАНИЯ* – это комбинация двух причин, описанных выше: *нарушение ЗОНАЛЬНОСТИ* и *нарушение КОМИССИОНИРОВАНИЯ*;
- *нарушение ВРЕМЕНИ, ЗОНАЛЬНОСТИ и КОМИССИОНИРОВАНИЯ* – это комбинация трех причин, описанных выше: *нарушение ВРЕМЕНИ*, *нарушение ЗОНАЛЬНОСТИ* и *нарушение КОМИССИОНИРОВАНИЯ* ;
- *нарушение ВЕРИФИКАЦИИ* – в результате верификации предъявленного идентификатора, контроллером не было получено подтверждения от

верифицирующего устройства в данном направлении, но проход был осуществлен в другом направлении и по другому считывателю;

- *нарушение ВРЕМЕНИ и ВЕРИФИКАЦИИ* - в результате верификации предъявленного идентификатора, контроллером не было получено подтверждения от верифицирующего устройства в данном направлении, но проход был осуществлен с *нарушением ВРЕМЕНИ* в другом направлении и по другому считывателю;
- *нарушение ЗОНАЛЬНОСТИ и ВЕРИФИКАЦИИ* - в результате верификации предъявленного идентификатора, контроллером не было получено подтверждения от верифицирующего устройства в данном направлении, но проход был осуществлен с *нарушением ЗОНАЛЬНОСТИ* в другом направлении и по другому считывателю;
- *нарушение ВРЕМЕНИ, ЗОНАЛЬНОСТИ и ВЕРИФИКАЦИИ* - это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ и ВЕРИФИКАЦИИ* и *нарушение ЗОНАЛЬНОСТИ и ВЕРИФИКАЦИИ*;

Проход, подтверждение от ДУ – событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером с подтверждением от ДУ права прохода и до истечения времени удержания ИУ в открытом состоянии. Подтверждение от ДУ осуществляется при условии, что стоят опции «подтверждения от ДУ» для верификации сотрудников либо посетителей на каждый считыватель:

- при проходе
- при проходе с НАРУШЕНИЕМ ВРЕМЕНИ
- при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ

Проход с подтверждением от ДУ и причиной нарушения:

- *нарушение ВРЕМЕНИ* – предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* – предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение ЗОНАЛЬНОСТИ*;

Проход, подтверждение от ВЕРИФИКАЦИИ - событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером с подтверждением от верифицирующего устройства права прохода и до истечения времени удержания ИУ в открытом состоянии. Подтверждение от верифицирующего устройства осуществляется в соответствии с параметрами, задаваемыми в модуле «ВЕРИФИКАЦИЯ » для верификации сотрудников либо посетителей на каждый считыватель:

- при проходе;
- при проходе с НАРУШЕНИЕМ ВРЕМЕНИ;
- при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ ;

Проход с подтверждением от ВЕРИФИКАЦИИ и причиной нарушения:

- *нарушение ВРЕМЕНИ* – предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* – предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;

- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение ЗОНАЛЬНОСТИ*;

ИУ не закрыто после прохода (с фиксацией номера идентификатора). Событие возникает, если после прохода по идентификатору время активизации состояния контакта ИУ превысило установленное предельное время разблокировки. То есть, например, после открытия дверь остается в открытом состоянии в течение времени большем, чем время удержания в открытом состоянии, установленное для данного контроллера.

Проход по команде от ДУ. Событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером по команде от ДУ права прохода и до истечения времени удержания ИУ в открытом состоянии.

Проход по команде от ПК. Событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером по команде от ПК права прохода и до истечения времени удержания ИУ в открытом состоянии.

Проход по команде от ИК - пульта. Событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером по команде от ИК - пульта права прохода и до истечения времени удержания ИУ в открытом состоянии.

Несанкционированный проход через ИУ (взлом ИУ). Событие, возникающее при активизации состояния контакта ИУ, не сопровождающегося санкционированным системой открытием ИУ. Механической разблокировки двери, турникета с последующим проходом через него.

События, связанные с изменением текущего состояния дополнительных выходов

Активизация выхода. Событие происходит в случае подачи контроллером управляющего сигнала на дополнительный выход. Причиной может служить команда от программного обеспечения или выполнение заданной на этапе конфигурации логики работы контроллера.

Нормализация выхода. Событие происходит в случае снятия контроллером управляющего сигнала с дополнительного выхода. Причиной может служить команда от программного обеспечения или выполнение заданной на этапе конфигурации логики работы контроллера.

Запуск задержки активизации выхода. Только для выхода типа «ОПС». Событие происходит в случае подачи контроллером управляющего сигнала на дополнительный выход, если параметр выхода «Задержка перед запуском» не равен 0. Причиной может служить команда от программного обеспечения или выполнение заданной на этапе конфигурации логики работы контроллера.

КЗ на выходе. Событие происходит только для дополнительного выхода типа «ОПС» с номером 5 или 6, в если на выходе обнаружено короткое замыкание.

Обрыв на выходе. Событие происходит только для дополнительного выхода типа «ОПС» с номером 5 или 6, если на выходе обнаружен обрыв.

Активизация выхода невозможна, КЗ. Событие происходит только для дополнительного выхода типа «ОПС» с номером 5 или 6, если на выходе обнаружено короткое замыкание при попытке контроллера подать управляющий сигнал на данный выход.

Восстановление выхода. Событие происходит только для дополнительного выхода типа «ОПС» с номером 5 или 6, если после сброса контроллера на выходе не обнаружены никакие неисправности.

События, связанные с изменением текущего состояния корпуса контроллера

Корпус контроллера открыт. Событие происходит в случае вскрытия корпуса контроллера.

Корпус контроллера закрыт. Событие происходит при закрытии корпуса контроллера.

События, связанные с работоспособностью сетевых каналов контроллера

Система безопасности взаимодействует с любым контроллером по 3 сетевым каналам. Для нормальной работы контроллера требуется, чтобы все 3 сетевых канала были открыты:

- канал управления — служит для передачи команд управления от системы безопасности к контроллеру. С данным каналом связаны следующие события:
 - *Канал управления ОТКРЫТ* — событие возникает при открытии канала управления сервером системы;
 - *Канал управления ЗАКРЫТ* — событие возникает при закрытии канала управления сервером системы;
 - *Канал управления НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала управления сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу управления другим программным обеспечением (например, локальным ПО);
 - *Канал управления неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом управления контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;
 - *Канал управления НЕ АВТОРИЗИРОВАН* — событие возникает при невозможности сервера системы получить авторизованный доступ к контроллеру. Причиной, вызывающей такое событие, является наличие установленного пароля в контроллере, отличного от передаваемого пароля на этот контроллер системой безопасности;
 - *Ожидание открытия канала управления*- событие возникает при постановке в очередь сервера системы запроса на открытие канала управления;
 - *Отмена ожидания открытия канала управления*- событие возникает при удалении из очереди сервера системы запроса на открытие канала управления;
 - *Попытка открытия канала управления* — событие уведомляет о начале операции по открытию канала управления сервером системы;

- *Нарушение связи с каналом управления* — событие возникает при отсутствии связи между сервером системы и каналом управления контроллера в течении 2 мин.;
- *Нет ответа на выполнение команды по каналу управления* — событие возникает в случае отсутствия ответа от контроллера в течении 6 мин. на выполнение команды сервером системы;
- канал мониторинга — служит для получения системой безопасности журнала мониторинга контроллера. С данным каналом связаны следующие события:
 - *Канал мониторинга ОТКРЫТ* — событие возникает при открытии канала мониторинга сервером системы;
 - *Канал мониторинга ЗАКРЫТ* — событие возникает при закрытии канала мониторинга сервером системы;
 - *Канал мониторинга НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала мониторинга сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу мониторинга другим программным обеспечением (например, локальным ПО);
 - *Канал мониторинга неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом мониторинга контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;
 - *Попытка открытия канала мониторинга* — событие уведомляет о начале операции по открытию канала мониторинга сервером системы;
 - *Нарушение связи с каналом мониторинга* — событие возникает при отсутствии связи между сервером системы и каналом мониторинга контроллера в течении 2 мин.;
- канал регистрации - служит для получения системой безопасности журнала регистрации контроллера. С данным каналом связаны следующие события:
 - *Канал регистрации ОТКРЫТ* — событие возникает при открытии канала регистрации сервером системы;
 - *Канал регистрации ЗАКРЫТ* — событие возникает при закрытии канала регистрации сервером системы;
 - *Канал регистрации НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала регистрации сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу регистрации другим программным обеспечением (например, локальным ПО);
 - *Канал регистрации неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом регистрации контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;
 - *Попытка открытия канала регистрации* — событие уведомляет о начале операции по открытию канала регистрации сервером системы;
 - *Нарушение связи с каналом регистрации* — событие возникает при отсутствии связи между сервером системы и каналом регистрации контроллера в течении 2 мин.;

События, связанные с изменением текущего состояния контроллеров или системы

Включение или выключение питания контроллера. Выключение питания может возникнуть в двух случаях: или при штатном выключении блока питания контроллера, или при аварийном выключении, связанным с аварией сети и разрядом аккумулятора. Включение питания возникает аналогично выключению в двух случаях: или при штатном включении блока питания контроллера, или при восстановлении сетевого питания.

Нарушение или восстановление связи с контроллером. Эти события относятся к разряду диагностических и отражают возможное нарушение и восстановление работоспособности структурных элементов системы. Такие события возникают при нарушении связи между программным обеспечением системы безопасности и контроллером. Через 2 минуты отсутствия связи по одному из каналов контроллера, соединение по всем каналам будет закрыто. События генерируется при нарушении связи с

- каналом управления;
- каналом мониторинга;
- каналом регистрации;

Переполнение или очистка журнала регистрации. Переполнение журнала возникает после заполнения в памяти контроллера свободной предпоследней страницы журнала (размер одной страницы равен 32 событиям). Очистка журнала происходит всегда после чтения переполненного журнала регистрации.

Переполнение списка идентификаторов. Событие появляется в случае, если из-за внутренней ошибки программного обеспечения в контроллер передано количество карт доступа, превышающее его ресурсы.

Ошибка принятого сообщения. Событие возникает в случае невозможности контроллера правильно декодировать принятые от программного обеспечения сообщения. Может быть вызвано ошибками сети Ethernet.

Сбой физического уровня Ethernet. Событие происходит в случае обнаружения внутренних ошибок в сети Ethernet.

Перезапуск контроллера. Событие возникает в случае решения контроллера о поведении аппаратного сброса. Данные события носят диагностический характер:

- внешний сброс;
- сброс по WatchDog.

Неисправность контроллера. Приведенные ниже события носят диагностический характер и содержат информацию о выходе из строя составляющих контроллера:

- памяти FRAM;
- памяти DataFlash;
- памяти SRAM;
- часов RTC;
- шины I²C;
- ошибки сопроцессора;

Форматирование памяти событий. Приведенные ниже события содержат информацию об изменении состояния внутренней памяти контроллера и носят диагностический характер:

- *область журнала событий;*
- *область списка карт;*
- *область установок конфигурации;*
- *область программ;*
- *область текущих установок.*

Изменение режима работы (РР) по команде от ПО (только для КБО). Событие возникает при изменении режима работы оператором из программного обеспечения.

Установлен режим работы "Открыто" по команде от ПЗ (только для КБО). Событие возникает при установке режима работы «Открыто», если пожарная зона перешла в режим «ПОЖАР» или «ВНИМАНИЕ».

Изменение РР на/с РР «Охрана» (только для КБО). Событие возникает при постановке/снятии с охраны охранной зоны, в которую входит ИУ. Выход из РР «Охрана» производится в РР «Контроль».

Изменение РР по команде от ИК (только для КБО). Событие регистрируется при смене режима контроля доступа в результате команды получаемой контроллером управления доступом от ИК пульта управления.

Тревога по команде от ИК-пульта (только для КБО). Событие регистрируется при получении команды поднятия тревоги от ИК пульта управления..

Авария или восстановление питания. Авария возникает в случае понижения напряжения питания контроллера ниже уровня 10 вольт. Восстановление происходит в случае установления нормального уровня напряжения в 12 вольт.

Тревога или сброс тревоги по команде от ПО (только для КБО). События связаны с возникновением тревожной ситуации в системе (см. параметры генератора тревоги) и сбросом сигнала тревоги оператором системы под управлением ПО "Управление системой" или активизацией дополнительного входа сброса тревоги.

Автономный сброс тревоги по кнопке. Событие возникает при нажатии на кнопку «СБРОС» на БУИ.

Автономное отключение звука по кнопке. Событие возникает при нажатии на кнопку «ОТКЛ ЗВУКА» на БУИ.

Переход на резерв ИП. Событие возникает при активизации входа «Переход на РИП», подключенного к резервному источнику питания.

Разряд батареи ИП. Событие возникает при активирован вход «Разряд ИП» или напряжение питания менее 10.5 В при активизированном входе «Переход на РИП».

Утечка на землю в ШС. Событие возникает при условии, что сопротивление между цепью GND на плате контроллера и «землей» меньше 20 кОм.

Восстановление после утечки на землю в ШС. Событие возникает при условии, что сопротивление между цепью GND на плате контроллера и «землём» больше 20 кОм.

Кнопки заблокированы. Событие возникает через 20 с после последнего нажатия на любую кнопку БУИ, при условии, что кнопки БУИ были разблокированы.

Кнопки разблокированы. Событие возникает после выполнения последовательности действий, приводящих к разблокировке кнопок БУИ.

Сброс от кнопки запущен. Событие возникает при начале процедуры сброса, инициированной нажатием на кнопку «СБРОС» на БУИ.

Сброс по команде от ПО запущен. Событие возникает при начале процедуры сброса, инициированной командой оператора от ПО.

Нарушение или восстановление связи с БУИ. События возникают при нарушении или восстановлении связи с БУИ.

Неисправность ИП +18В. Событие возникает в случае выхода напряжения питания ШС за рабочий диапазон.

Восстановление ИП +18В. Событие возникает в случае возврата напряжения питания ШС в рабочий диапазон.

События, связанные с изменениями состояний зон

ОЗ взята на охрану. Событие возникает при переходе охранной зоны (ОЗ) в режим «ОХРАНА». Если с ОЗ связано ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Охрана». Имеются следующие уточнения:

- *по идентификатору* - если идентификатор имеет соответствующие права.
- *по идентификатору, подтверждение от ВЕРИФИКАЦИИ* - если было подтверждения от верифицирующего устройства.
- *по команде от ПО* - после выполнения команды оператором ПО.
- *по кнопке* - по кнопке на БУИ;

ОЗ снята с охраны. Событие возникает при переходе охранной зоны (ОЗ) в режим «СНЯТА». Если с ОЗ связано ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Контроль». Имеются следующие уточнения:

- *по идентификатору* - если идентификатор имеет соответствующие права;
- *по идентификатору, подтверждение от ВЕРИФИКАЦИИ* - если было подтверждения от верифицирующего устройства;
- *по команде от ПО* - после выполнения команды оператором ПО.

по кнопке - по кнопке на БУИ;

- *по команде от ПЗ* — если пожарная зона (ПЗ) перешла в режим «ПОЖАР» или «ВНИМАНИЕ». Конкретное условия снятия ОЗ с охраны зависит от значения параметра ПЗ **Переводить ИУ в режим «Открыто»** ;

Попытка взятия ОЗ на охрану (невозможно взять) по идентификатору. Событие возникает при попытке взятия охранной зоны на охрану по идентификатору :

- *нарушение состояния ИУ.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ИУ, связанного с этой ОЗ, было не нормализовано. Например, это может происходить при постановке на охрану при открытой двери;
- *нарушение состояния ШС.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ШС, включенного в эту ОЗ, было не нормализовано;
- *нарушение КОМИССИОНИРОВАНИЯ.* Событие возникает, если в процессе взятия ОЗ на охрану было зафиксировано несоответствие с комиссионировавшим идентификатором или комиссионирование не было выполнено вообще;
- *нарушение ВЕРИФИКАЦИИ.* Событие возникает, если в процессе взятия ОЗ на охрану не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *нарушение ВРЕМЕНИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану и являющегося нарушителем по времени;
- *нарушение ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану и являющегося нарушителем зональности;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану и являющегося нарушителем и по времени и зональности;
- *отказ от постановки.* Событие возникает, если после поднесения к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану и до истечения времени удержания ИУ в открытом состоянии, этот идентификатор не был поднесен повторно.

Попытка снятия ОЗ с охраны (невозможно снять) по идентификатору. Событие возникает при попытке снятия ОЗ с охраны по идентификатору:

- *нарушение КОМИССИОНИРОВАНИЯ.* Событие возникает, если в процессе снятия ОЗ с охраны было зафиксировано несоответствие с комиссионировавшим идентификатором или комиссионирование не было выполнено вообще;
- *нарушение ВЕРИФИКАЦИИ.* Событие возникает, если в процессе снятия ОЗ с охраны не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *нарушение ВРЕМЕНИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны и являющегося нарушителем по времени;
- *нарушение ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны и являющегося нарушителем зональности;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны любой группы ресурсов и являющегося нарушителем и по времени и по зональности;
- *отказ от снятия.* Событие возникает, если после поднесения к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны любой и до истечения времени удержания ИУ в открытом состоянии, этот идентификатор не был поднесен повторно.

Попытка взятия ОЗ на охрану (невозможно взять) по команде от ПО. Событие возникает при попытке взятия охранной зоны на охрану по команде от оператора ПО :

- *нарушение состояния ИУ.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ИУ, связанного с этой ОЗ, было не нормализовано. Например, это может происходить при постановке на охрану при открытой двери;
- *нарушение состояния ШС.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ШС, включенного в эту ОЗ, было не нормализовано;

Попытка взятия ОЗ на охрану (невозможно взять) по кнопке. Событие возникает при попытке взятия охранной зоны на охрану по кнопке на БУИ :

- *нарушение состояния ИУ.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ИУ, связанного с этой ОЗ, было не нормализовано. Например, это может происходить при постановке на охрану при открытой двери;
- *нарушение состояния ШС.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ШС, включенного в эту ОЗ, было не нормализовано;

Тихая тревога по ОЗ. Событие возникает при переходе ОЗ в режим «ТРЕВОГА» (при нарушении любого ОШС) и если установлен параметр конфигурации зоны **Не активизировать при тревоге по Охранным шлейфам сигнализации выходы, работающие по программам «Сирена» и «Лампа».**

Тревога по ОЗ. Событие возникает при переходе ОЗ в режим «ТРЕВОГА» (при нарушении любого ОШС) и если не установлен параметр конфигурации зоны **Не активизировать при тревоге по Охранным шлейфам сигнализации выходы, работающие по программам «Сирена» и «Лампа».**

Сброс тревоги по ОЗ по команде от ПО. Событие возникает при сбросе тревоги на ОЗ по команде оператора от ПО. Причем ОЗ режим не меняет, а индикация на БУИ для нарушенных ОШС этой зоны будет отличаться от нормализованных

Взятие ОЗ на охрану. Событие возникает при попытке перехода охранной зоны (ОЗ) в режим «ОХРАНА». Имеются следующие уточнения:

- *по идентификатору* - если идентификатор имеет соответствующие права;
- *по команде от ПО* - по команде от оператора ПО;
- *по кнопке* - по кнопке на БУИ;

ПЗ снята с контроля. Событие возникает при снятии с контроля ПЗ и переходе ее в режим «СНЯТА». Имеются следующие уточнения:

- *по команде от ПО* - по команде от оператора ПО;
- *по кнопке* по кнопке на БУИ;

ПЗ взята на контроль. Событие возникает при взятии на контроля ПЗ и переходе ее в режим «НОРМА». Имеются следующие уточнения:

- *по команде от ПО* - по команде от оператора ПО;
- *по кнопке* - по кнопке на БУИ;

ПЗ перешла в режим. Событие возникает при переходе ПЗ в конкретный режим. Имеются следующие уточнения:

- «Неисправность» - ПЗ перешла в режим «Неисправность»;
- «Внимание» - ПЗ перешла в режим «Внимание»;
- «Пожар» - ПЗ перешла в режим «Пожар»;
- «Норма» - ПЗ перешла в режим «Норма» после сброса из одного из режимов: «Неисправность», «Внимание» или «Пожар»;

События, связанные с изменением текущего состояния ШС, входящих в ОЗ и ПЗ

ОШС не взят на охрану, переход в режим "Автоперевзятие". Событие возникает, если в момент взятия ШС на охрану его состояние окажется не нормализованным. ШС перейдет в состояние «Автоперевзятие».

ОШС взят на охрану. Событие возникает, если ОШС перешел в режим «ОХРАНА».

ОШС снят с охраны. Событие возникает, если ОШС перешел в режим «СНЯТ».

Взятие ОШС на охрану. Событие возникает при переходе ОШС в режим «ВЗЯТИЕ».

ПШС отключен. Событие возникает, если была передана новая конфигурация на ПШС, указывающая не использовать данный ПШС.

ОШС отключен. Событие возникает, если была передана новая конфигурация на ПШС, указывающая не использовать данный ОШС.

Корпус извещателя вскрыт (ОШС). Событие возникает, если на одном из охранных извещателей вскрыт корпус .

Корпус извещателя закрыт (ОШС). Событие возникает, если на одном из извещателей корпус закрыт после вскрытия.

Неисправность снятого ОШС. Событие возникает, если происходит нарушения ОШС в режиме «СНЯТ» и параметр конфигурации ОШС **Задержка восстановления нарушенного ОШС в снятом состоянии** отличен от нуля.

Нормализация снятого ОШС. Событие возникает, если происходит нормализация ОШС в режиме «СНЯТ» и параметр конфигурации ОШС **Задержка восстановления нарушенного ОШС в снятом состоянии** отличен от нуля..

Нарушение ОШС, переход в режим "Тревога". Событие возникает, если ОШС перешел в режим «ТРЕВОГА».

Нарушение ОШС, переход в режим "Тихая тревога". Событие возникает, если ОШС перешел в режим «ТРЕВОГА», а в ОЗ, включающей данный шлейф, установлен параметр конфигурации **Не активизировать при тревоге по Охранным шлейфам сигнализации выходы, работающие по программам «Сирена» и «Лампа».**

Нарушение ОШС в режиме "Тревога". Событие возникает, если происходит повторное нарушение ОШС в режиме «ТРЕВОГА».

Восстановление ОШС в режиме "Тревога". Событие возникает, если происходит восстановление нарушенного ОШС в режиме «ТРЕВОГА».

Сброс тревоги ОШС. Событие возникает при сбросе тревоги на ОЗ, включающей данный ОШС.

ПШС перешел в режим "Норма". Событие возникает, если ПШС перешел в режим «НОРМА».

Неисправность ПШС, КЗ. Событие возникает, если ПШС перешел в состояние «НЕИСПРАВНОСТЬ» по причине короткого замыкания.

Неисправность ПШС, обрыв. Событие возникает, если ПШС перешел в состояние «НЕИСПРАВНОСТЬ» по причине обрыва.

ПШС, сработал 1 извещатель. Событие возникает, если на ПШС сработал один извещатель.

ПШС, сработало 2 извещателя. Событие возникает, если на ПШС сработало два или более извещателей .

Сброс ПШС по команде от ПО. Событие возникает, если осуществлен сброс ПШС по команде оператора от ПО.

Сброс ПШС по кнопке. Событие возникает, если осуществлен сброс ПШС по кнопке от БУИ.

Сброс ПШС при перезапросе. Событие возникает, если .

ПШС взят на контроль. Событие возникает, если ПШС перешел в режим «ВЗЯТ».

ПШС снят с контроля. Событие возникает, если ПШС перешел в режим «СНЯТ».

Взятие ПШС на контроль. Событие возникает, если .

ПШС перешел в режим "Внимание". Событие возникает, если ПШС перешел в режим «ВНИМАНИЕ».

ПШС перешел в режим "Пожар". Событие возникает, если ПШС перешел в режим «ПОЖАР».

События, связанные с изменением текущего состояния ИУ, входящих в ОЗ

ИУ взят на охрану. Событие возникает, если ОЗ перешла в режим «ОХРАНА».

ИУ снят с охраны. Событие возникает, если ОЗ перешла в режим «СНЯТА».

Нарушение ИУ, переход в режим "Тревога". Событие возникает, если ОЗ перешла в режим «ТРЕВОГА» из-за несанкционированной разблокировки ИУ.

Сброс тревоги ИУ. Событие возникает при снятии ОЗ с охраны, если она до этого находилась в режиме «ТРЕВОГА».

События контроллера доступа (серия СТ/L04)

События, связанные с перемещением через ИУ

Запрет прохода с причиной:

- *идентификатор НЕ ЗАРЕГИСТРИРОВАН* – предъявленный идентификатор никогда не передавался в контроллер, то есть ему не назначались права доступа в этот контроллер;
- *идентификатор ЗАПРЕЩЁН* - доступ предъявленному идентификатора явным образом запрещен в контроллере, то есть данный контроллер включен в список доступа предъявленного идентификатора с явным запрещением проходов;
- *идентификатор из СТОП-ЛИСТА* - предъявленный идентификатор занесен в «СТОП-ЛИСТ»;
- *идентификатор ПРОСРОЧЕН* — у предъявленного идентификатора истек срок действия, указанный в параметрах доступа;
- *нарушение ВРЕМЕНИ* - у данного контроллера установлен «жесткий» контроль времени, а предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* - у данного контроллера установлена «жесткая» защита от передачи идентификаторов, а предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* - это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение ЗОНАЛЬНОСТИ*;
- *нарушение КОМИССИОНИРОВАНИЯ* - было зафиксировано несоответствие с комиссионировавшим идентификатором или комиссионирование не было выполнено вообще;
- *запрет по команде от ДУ* - охранник пультом ДУ подал команду на запрет прохода, после того, как контроллер разрешил проход;
- *запрет по команде от ПО* - оператор с ПК подал команду на запрет прохода, после того, как контроллер разрешил проход;
- *отказ в подтверждении от ВЕРИФИКАЦИИ* - не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *нарушение РЕЖИМОВ РАБОТЫ* – у данного контроллера установлен такой режим работы, при котором доступ по предъявленному идентификатору запрещен (режимы «ЗАКРЫТО» и «ОХРАНА»);

Отказ от прохода - отказ от предоставленного системой права пройти через ИУ по идентификатору.

Проход — событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером права пройти через него и до истечения времени удержания ИУ в открытом состоянии, без каких-либо выявленных нарушений.

Проход с причиной нарушения:

- *нарушение ВРЕМЕНИ* – у данного контроллера установлен «мягкий» контроль времени, а предъявленный идентификатор не удовлетворяет указанному в правах доступа временному критерию доступа;
- *нарушение ЗОНАЛЬНОСТИ* – у данного контроллера установлена «мягкая» защита от передачи идентификаторов, а предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение ЗОНАЛЬНОСТИ*;
- *нарушение КОМИССИОНИРОВАНИЯ* – было зафиксировано несоответствие с комиссионировающим идентификатором или комиссионирование не было выполнено вообще;
- *нарушение ВРЕМЕНИ и КОМИССИОНИРОВАНИЯ* – это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ* и *нарушение КОМИССИОНИРОВАНИЯ*;
- *нарушение ЗОНАЛЬНОСТИ и КОМИССИОНИРОВАНИЯ* – это комбинация двух причин, описанных выше: *нарушение ЗОНАЛЬНОСТИ* и *нарушение КОМИССИОНИРОВАНИЯ*;
- *нарушение ВРЕМЕНИ, ЗОНАЛЬНОСТИ и КОМИССИОНИРОВАНИЯ* – это комбинация трех причин, описанных выше: *нарушение ВРЕМЕНИ*, *нарушение ЗОНАЛЬНОСТИ* и *нарушение КОМИССИОНИРОВАНИЯ* ;
- *нарушение ВЕРИФИКАЦИИ* – в результате верификации предъявленного идентификатора, контроллером не было получено подтверждения от верифицирующего устройства в данном направлении, но проход был осуществлен в другом направлении и по другому считывателю;
- *нарушение ВРЕМЕНИ и ВЕРИФИКАЦИИ* - в результате верификации предъявленного идентификатора, контроллером не было получено подтверждения от верифицирующего устройства в данном направлении, но проход был осуществлен с *нарушением ВРЕМЕНИ* в другом направлении и по другому считывателю;
- *нарушение ЗОНАЛЬНОСТИ и ВЕРИФИКАЦИИ* - в результате верификации предъявленного идентификатора, контроллером не было получено подтверждения от верифицирующего устройства в данном направлении, но проход был осуществлен с *нарушением ЗОНАЛЬНОСТИ* в другом направлении и по другому считывателю;
- *нарушение ВРЕМЕНИ, ЗОНАЛЬНОСТИ и ВЕРИФИКАЦИИ* - это комбинация двух причин, описанных выше: *нарушение ВРЕМЕНИ и ВЕРИФИКАЦИИ* и *нарушение ЗОНАЛЬНОСТИ и ВЕРИФИКАЦИИ*;

Проход, подтверждение от ДУ – событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером с подтверждением от ДУ права прохода и до истечения времени удержания ИУ в открытом состоянии. Подтверждение от ДУ осуществляется при условии, что стоят опции «подтверждения от ДУ» для верификации сотрудников либо посетителей на каждый считыватель:

- при проходе
- при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ

Проход с подтверждением от ДУ и причиной нарушения:

- *нарушение ЗОНАЛЬНОСТИ* – предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;

Проход, подтверждение от ВЕРИФИКАЦИИ - событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером с подтверждением от верифицирующего устройства права прохода и до истечения времени удержания ИУ в открытом состоянии. Подтверждение от верифицирующего устройства осуществляется в соответствии с параметрами, задаваемыми в разделе «ВЕРИФИКАЦИЯ » для верификации сотрудников на каждый считыватель:

- *при проходе;*
- *при проходе с НАРУШЕНИЕМ ЗОНАЛЬНОСТИ ;*

Проход с подтверждением от ВЕРИФИКАЦИИ и причиной нарушения:

- *нарушение ЗОНАЛЬНОСТИ* – предъявленный идентификатор нарушил зональность, т.е. была совершена попытка повторного входа/выхода;

ИУ не закрыто после прохода (с фиксацией номера идентификатора). Событие возникает, если после прохода по идентификатору время активизации состояния контакта ИУ превысило установленное предельное время разблокировки. То есть, например, после открытия дверь остается в открытом состоянии в течение времени большим, чем время удержания в открытом состоянии, установленное для данного контроллера.

Проход по команде от ДУ. Событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером по команде от ДУ права прохода и до истечения времени удержания ИУ в открытом состоянии.

Проход по команде от ПК. Событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером по команде от ПК права прохода и до истечения времени удержания ИУ в открытом состоянии.

Проход по команде от ИК - пульта. Событие, возникающее при проходе через ИУ, произошедшем после предоставления контроллером по команде от ИК - пульта права прохода и до истечения времени удержания ИУ в открытом состоянии.

Несанкционированный проход через ИУ (взлом ИУ). Событие, возникающее при активизации состояния контакта ИУ, не сопровождающегося санкционированным системой открытием ИУ. Механической разблокировки двери, турникета с последующим проходом через него.

События, связанные с изменением текущего состояния дополнительных входов

Активизация входа - вызывается срабатыванием устройства, подключенного к данному дополнительному входу.

Нормализация входа – вызывается отключением устройства (переходом в нормальное состояние), подключенного к данному дополнительному входу.

События, связанные с изменением текущего состояния дополнительных выходов

Активизация выхода. Событие происходит в случае подачи контроллером управляющего сигнала на дополнительный выход. Причиной может служить команда от программного обеспечения или выполнение заданной на этапе конфигурации логики работы контроллера.

Нормализация выхода. Событие происходит в случае снятия контроллером управляющего сигнала с дополнительного выхода. Причиной может служить команда от программного обеспечения или выполнение заданной на этапе конфигурации логики работы контроллера.

Запуск задержки активизации выхода. Только для выхода типа «ОПС». Событие происходит в случае подачи контроллером управляющего сигнала на дополнительный выход, если параметр выхода «Задержка перед запуском» не равен 0. Причиной может служить команда от программного обеспечения или выполнение заданной на этапе конфигурации логики работы контроллера.

КЗ на выходе. Событие происходит только для дополнительного выхода типа «ОПС» с номером 5 или 6, в если на выходе обнаружено короткое замыкание.

Обрыв на выходе. Событие происходит только для дополнительного выхода типа «ОПС» с номером 5 или 6, если на выходе обнаружен обрыв.

Активизация выхода невозможна, КЗ. Событие происходит только для дополнительного выхода типа «ОПС» с номером 5 или 6, если на выходе обнаружено короткое замыкание при попытке контроллера подать управляющий сигнал на данный выход.

Восстановление выхода. Событие происходит только для дополнительного выхода типа «ОПС» с номером 5 или 6, если после сброса контроллера на выходе не обнаружены никакие неисправности.

События, связанные с изменением текущего состояния корпуса контроллера

Корпус контроллера открыт. Событие происходит в случае вскрытия корпуса контроллера.

Корпус контроллера закрыт. Событие происходит при закрытии корпуса контроллера.

События, связанные с работоспособностью сетевых каналов контроллера

Система безопасности взаимодействует с любым контроллером по 3 сетевым каналам. Для нормальной работы контроллера требуется, что бы все 3 сетевых канала были открыты:

- канал управления — служит для передачи команд управления от системы безопасности к контроллеру. С данным каналом связаны следующие события:

- *Канал управления ОТКРЫТ* — событие возникает при открытии канала управления сервером системы;
 - *Канал управления ЗАКРЫТ* — событие возникает при закрытии канала управления сервером системы;
 - *Канал управления НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала управления сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу управления другим программным обеспечением (например, локальным ПО);
 - *Канал управления неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом управления контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;
 - *Канал управления НЕ АВТОРИЗИРОВАН* — событие возникает при невозможности сервера системы получить авторизованный доступ к контроллеру. Причиной, вызывающей такое событие, является наличие установленного пароля в контроллере, отличного от передаваемого пароля на этот контроллер системой безопасности;
 - *Ожидаемый тип контроллера не соответствует заданному* — событие возникает при невозможности сервера системы продолжать работу с контроллером, тип конфигурации которого в системе безопасности отличается от типа, выставленного переключками на его системной плате;
 - *Ожидание открытия канала управления* — событие возникает при постановке в очередь сервера системы запроса на открытие канала управления;
 - *Отмена ожидания открытия канала управления* — событие возникает при удалении из очереди сервера системы запроса на открытие канала управления;
 - *Попытка открытия канала управления* — событие уведомляет о начале операции по открытию канала управления сервером системы;
 - *Нарушение связи с каналом управления* — событие возникает при отсутствии связи между сервером системы и каналом управления контроллера в течении 2 мин.;
 - *Нет ответа на выполнение команды по каналу управления* — событие возникает в случае отсутствия ответа от контроллера в течении 6 мин. на выполнение команды сервером системы;
-
- канал мониторинга — служит для получения системой безопасности журнала мониторинга контроллера. С данным каналом связаны следующие события:
 - *Канал мониторинга ОТКРЫТ* — событие возникает при открытии канала мониторинга сервером системы;
 - *Канал мониторинга ЗАКРЫТ* — событие возникает при закрытии канала мониторинга сервером системы;
 - *Канал мониторинга НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала мониторинга сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу мониторинга другим программным обеспечением (например, локальным ПО);
 - *Канал мониторинга неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом мониторинга контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;

- *Попытка открытия канала мониторинга* — событие уведомляет о начале операции по открытию канала мониторинга сервером системы;
 - *Нарушение связи с каналом мониторинга* — событие возникает при отсутствии связи между сервером системы и каналом мониторинга контроллера в течении 2 мин.;
- канал регистрации - служит для получения системой безопасности журнала регистрации контроллера. С данным каналом связаны следующие события:
- *Канал регистрации ОТКРЫТ* — событие возникает при открытии канала регистрации сервером системы;
 - *Канал регистрации ЗАКРЫТ* — событие возникает при закрытии канала регистрации сервером системы;
 - *Канал регистрации НЕ ОТКРЫТ* — событие возникает при невозможности открытия канала регистрации сервером системы. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо наличие установленной связи по каналу регистрации другим программным обеспечением (например, локальным ПО);
 - *Канал регистрации неожиданно был ЗАКРЫТ* — событие возникает при неожиданном разрыве связи между сервером системы и каналом регистрации контроллера. Причиной, вызывающей такое событие, может быть физическое отсутствие связи с контроллером в сети либо проблемы с контроллером;
 - *Попытка открытия канала регистрации* — событие уведомляет о начале операции по открытию канала регистрации сервером системы;
 - *Нарушение связи с каналом регистрации* — событие возникает при отсутствии связи между сервером системы и каналом регистрации контроллера в течении 2 мин.;

События, связанные с изменением текущего состояния контроллеров или системы

Включение или выключение питания контроллера. Выключение питания может возникнуть в двух случаях: или при штатном выключении блока питания контроллера, или при аварийном выключении, связанным с аварией сети и разрядом аккумулятора. Включение питания возникает аналогично выключению в двух случаях: или при штатном включении блока питания контроллера, или при восстановлении сетевого питания.

Нарушение или восстановление связи с контроллером. Эти события относятся к разряду диагностических и отражают возможное нарушение и восстановление работоспособности структурных элементов системы. Такие события возникают при нарушении связи между программным обеспечением системы безопасности и контроллером. Через 2 минуты отсутствия связи по одному из каналов контроллера, соединение по всем каналам будет закрыто. События генерируется при нарушении связи с

- каналом управления;
- каналом мониторинга;
- каналом регистрации;

Переполнение или очистка журнала регистрации. Переполнение журнала возникает после заполнения в памяти контроллера свободной предпоследней страницы журнала (размер

одной страницы равен 32 событиям). Очистка журнала происходит всегда после чтения переполненного журнала регистрации.

Переполнение списка идентификаторов. Событие появляется в случае, если из-за внутренней ошибки программного обеспечения в контроллер передано количество карт доступа, превышающее его ресурсы.

Ошибка принятого сообщения. Событие возникает в случае невозможности контроллера правильно декодировать принятые от программного обеспечения сообщения. Может быть вызвано ошибками сети Ethernet.

Сбой физического уровня Ethernet. Событие происходит в случае обнаружения внутренних ошибок в сети Ethernet.

Перезапуск контроллера. Событие возникает в случае решения контроллера о поведении аппаратного сброса. Данные события носят диагностический характер:

- *внешний сброс;*
- *сброс по WatchDog.*

Неисправность контроллера. Приведенные ниже события носят диагностический характер и содержат информацию о выходе из строя составляющих контроллера:

- *памяти FRAM;*
- *памяти DataFlash;*
- *памяти SRAM;*
- *часов RTC;*
- *шины I²C;*

Форматирование памяти событий. Приведенные ниже события содержат информацию об изменении состояния внутренней памяти контроллера и носят диагностический характер:

- *область журнала событий;*
- *область списка карт;*
- *область установок конфигурации;*
- *область программ;*
- *область прошивки;*
- *область текущих установок.*

Тревога по команде от ИК-пульта (только для КБО). Событие регистрируется при получении команды поднятия тревоги от ИК пульта управления..

Авария или восстановление питания. Авария возникает в случае понижения напряжения питания контроллера ниже уровня 10 вольт. Восстановление происходит в случае установления нормального уровня напряжения в 12 вольт.

Тревога или сброс тревоги по команде от ПО. События связаны с возникновением тревожной ситуации в системе (см. параметры генератора тревоги) и сбросом сигнала тревоги оператором системы под управлением ПО "Управление системой" или активизацией дополнительного входа сброса тревоги.

Автономный сброс тревоги по кнопке. Событие возникает при нажатии на кнопку «СБРОС».

Тестирование начато. Событие возникает при начале тестирования контроллера.

Тестирование завершено. Событие возникает при окончании тестирования контроллера.

Тестирование завершено, выявлены неисправности. Событие возникает при окончании тестирования контроллера в случае обнаружения каких-либо неисправностей.

Тестирование ШС начато. Событие возникает при начале тестирования шлейфа сигнализации.

Тестирование ШС завершено. Событие возникает при окончании тестирования шлейфа сигнализации.

Нарушение или восстановление связи с контроллером 2-го уровня. События возникают при нарушении или восстановлении связи с контроллером 2-го уровня.

Неисправность контроллера 2-го уровня. Событие возникает в случае неисправности одного из контроллеров 2-го уровня.

Восстановление после неисправности контроллера 2-го уровня. Событие возникает в случае восстановления после неисправности одного из контроллеров 2-го уровня.

Восстановление ИП +18В. Событие возникает в случае возврата напряжения питания ШС в рабочий диапазон..

Неисправность ИП +18В. Событие возникает в случае выхода напряжения питания ШС за рабочий диапазон.

Восстановление ИП +18В. Событие возникает в случае возврата напряжения питания ШС в рабочий диапазон.

События, связанные с изменениями состояний зон

ОЗ взята на охрану. Событие возникает при переходе охранной зоны (ОЗ) в режим «ОХРАНА». Если с ОЗ связано ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Охрана». Имеются следующие уточнения:

- *по идентификатору* - если идентификатор имеет соответствующие права.
- *по идентификатору, подтверждение от ВЕРИФИКАЦИИ* - если было подтверждения от верифицирующего устройства.
- *по команде от ПО* - после выполнения команды оператором ПО.
- *по кнопке* - по кнопке на БУИ;

ОЗ снята с охраны. Событие возникает при переходе охранной зоны (ОЗ) в режим «СНЯТА». Если с ОЗ связано ИУ, то данное событие будет сопровождаться событием «Смена РР на РР «Контроль». Имеются следующие уточнения:

- *по идентификатору* - если идентификатор имеет соответствующие права;

- *по идентификатору, подтверждение от ВЕРИФИКАЦИИ* - если было подтверждения от верифицирующего устройства;
- *по команде от ПО* - после выполнения команды оператором ПО.

по кнопке - по кнопке на БУИ;

- *по команде от ПЗ* — если пожарная зона (ПЗ) перешла в режим «ПОЖАР» или «ВНИМАНИЕ». Конкретное условия снятия ОЗ с охраны зависит от значения параметра ПЗ **Переводить ИУ в режим «Открыто»** ;

Попытка взятия ОЗ на охрану (невозможно взять) по идентификатору. Событие возникает при попытке взятия охранной зоны на охрану по идентификатору :

- *нарушение состояния ИУ.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ИУ, связанного с этой ОЗ, было не нормализовано. Например, это может происходить при постановке на охрану при открытой двери;
- *нарушение состояния ШС.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ШС, включенного в эту ОЗ, было не нормализовано;
- *нарушение КОМИССИОНИРОВАНИЯ.* Событие возникает, если в процессе взятия ОЗ на охрану было зафиксировано несоответствие с комиссионировающим идентификатором или комиссионирование не было выполнено вообще;
- *нарушение ВЕРИФИКАЦИИ.* Событие возникает, если в процессе взятия ОЗ на охрану не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *нарушение ВРЕМЕНИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану и являющегося нарушителем по времени;
- *нарушение ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану и являющегося нарушителем зональности;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану и являющуюся нарушителем и по времени и зональности;
- *отказ от постановки.* Событие возникает, если после поднесения к контроллеру, находящемуся в РР «Контроль», идентификатора с правами постановки на охрану и до истечения времени удержания ИУ в открытом состоянии, этот идентификатор не был поднесен повторно.

Попытка снятия ОЗ с охраны (невозможно снять) по идентификатору. Событие возникает при попытке снятия ОЗ с охраны по идентификатору:

- *нарушение КОМИССИОНИРОВАНИЯ.* Событие возникает, если в процессе снятия ОЗ с охраны было зафиксировано несоответствие с комиссионировающим идентификатором или комиссионирование не было выполнено вообще;
- *нарушение ВЕРИФИКАЦИИ.* Событие возникает, если в процессе снятия ОЗ с охраны не было подтверждения от верифицирующего устройства или верифицирующее устройство выдало запрет;
- *нарушение ВРЕМЕНИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны и являющегося нарушителем по времени;

- *нарушение ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны и являющегося нарушителем зональности;
- *нарушение ВРЕМЕНИ и ЗОНАЛЬНОСТИ.* Событие возникает при поднесении к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны любой группы ресурсов и являющегося нарушителем и по времени и по зональности;
- *отказ от снятия.* Событие возникает, если после поднесения к контроллеру, находящемуся в РР «Охрана», идентификатора с правами снятия с охраны любой и до истечения времени удержания ИУ в открытом состоянии, этот идентификатор не был поднесен повторно.

Попытка взятия ОЗ на охрану (невозможно взять) по команде от ПО. Событие возникает при попытке взятия охранной зоны на охрану по команде от оператора ПО :

- *нарушение состояния ИУ.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ИУ, связанного с этой ОЗ, было не нормализовано. Например, это может происходить при постановке на охрану при открытой двери;
- *нарушение состояния ШС.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ШС, включенного в эту ОЗ, было не нормализовано;

Попытка взятия ОЗ на охрану (невозможно взять) по кнопке. Событие возникает при попытке взятия охранной зоны на охрану по кнопке на БУИ :

- *нарушение состояния ИУ.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ИУ, связанного с этой ОЗ, было не нормализовано. Например, это может происходить при постановке на охрану при открытой двери;
- *нарушение состояния ШС.* Событие возникает, если в процессе взятия ОЗ на охрану состояние ШС, включенного в эту ОЗ, было не нормализовано;

Тихая тревога по ОЗ. Событие возникает при переходе ОЗ в режим «ТРЕВОГА» (при нарушении любого ОШС) и если установлен параметр конфигурации зоны **Не активизировать при тревоге по Охранным шлейфам сигнализации выходы, работающие по программам «Сирена» и «Лампа».**

Тревога по ОЗ. Событие возникает при переходе ОЗ в режим «ТРЕВОГА» (при нарушении любого ОШС) и если не установлен параметр конфигурации зоны **Не активизировать при тревоге по Охранным шлейфам сигнализации выходы, работающие по программам «Сирена» и «Лампа».**

Сброс тревоги по ОЗ по команде от ПО. Событие возникает при сбросе тревоги на ОЗ по команде оператора от ПО. Причем ОЗ режим не меняет, а индикация на БУИ для нарушенных ОШС этой зоны будет отличаться от нормализованных

Взятие ОЗ на охрану. Событие возникает при попытке перехода охранной зоны (ОЗ) в режим «ОХРАНА». Имеются следующие уточнения:

- *по идентификатору* - если идентификатор имеет соответствующие права;
- *по команде от ПО* - по команде от оператора ПО;
- *по кнопке* - по кнопке;

События, связанные с изменением текущего состояния ШС, входящих в ОЗ

ОШС не взят на охрану, переход в режим "Автоперевзятие". Событие возникает, если в момент взятия ШС на охрану его состояние окажется не нормализованным. ШС перейдет в состояние «Автоперевзятие».

ОШС взят на охрану. Событие возникает, если ОШС перешел в режим «ОХРАНА».

ОШС снят с охраны. Событие возникает, если ОШС перешел в режим «СНЯТ».

Взятие ОШС на охрану. Событие возникает при переходе ОШС в режим «ВЗЯТИЕ».

ОШС отключен. Событие возникает, если была передана новая конфигурация на ПШС, указывающая не использовать данный ОШС.

Корпус извещателя вскрыт (ОШС). Событие возникает, если на одном из охранных извещателей вскрыт корпус .

Корпус извещателя закрыт (ОШС). Событие возникает, если на одном из извещателей корпус закрыт после вскрытия.

Неисправность снятого ОШС. Событие возникает, если происходит нарушения ОШС в режиме «СНЯТ» и параметр конфигурации ОШС **Задержка восстановления нарушенного ОШС в снятом состоянии** отличен от нуля.

Нормализация снятого ОШС. Событие возникает, если происходит нормализация ОШС в режиме «СНЯТ» и параметр конфигурации ОШС **Задержка восстановления нарушенного ОШС в снятом состоянии** отличен от нуля..

Нарушение ОШС, переход в режим "Тревога". Событие возникает, если ОШС перешел в режим «ТРЕВОГА».

Нарушение ОШС, переход в режим "Тихая тревога". Событие возникает, если ОШС перешел в режим «ТРЕВОГА», а в ОЗ, включающей данный шлейф, установлен параметр конфигурации **Не активизировать при тревоге по Охранным шлейфам сигнализации выходы, работающие по программам «Сирена» и «Лампа».**

Нарушение ОШС в режиме "Тревога". Событие возникает, если происходит повторное нарушение ОШС в режиме «ТРЕВОГА».

Восстановление ОШС в режиме "Тревога". Событие возникает, если происходит восстановление нарушенного ОШС в режиме «ТРЕВОГА».

Сброс тревоги ОШС. Событие возникает при сбросе тревоги на ОЗ, включающей данный ОШС.

События, связанные с изменением текущего состояния ИУ, входящих в ОЗ

ИУ взят на охрану. Событие возникает, если ОЗ перешла в режим «ОХРАНА».

ИУ снят с охраны. Событие возникает, если ОЗ перешла в режим «СНЯТА».

Нарушение ИУ, переход в режим "Тревога". Событие возникает, если ОЗ перешла в режим «ТРЕВОГА» из-за несанкционированной разблокировки ИУ.

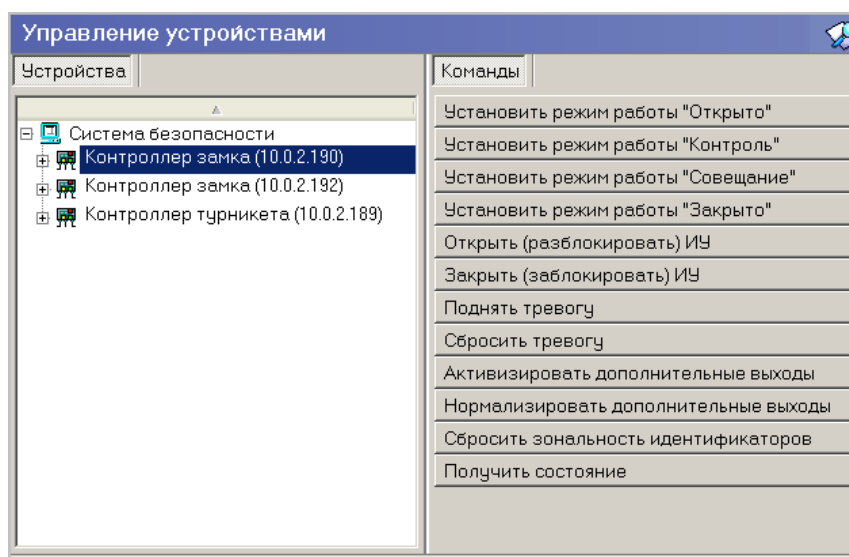
Сброс тревоги ИУ. Событие возникает при снятии ОЗ с охраны, если она до этого находилась в режиме «ТРЕВОГА».

КОМАНДЫ УПРАВЛЕНИЯ

Большинство устройств, входящих в единую систему безопасности PERCo-S-20, могут управляться из программного обеспечения. Для управления этими устройствами используются разделы Управление устройствами.

Ниже приведен список команд управления доступных для каждого типа устройств.

Контроллер управления доступом



- ✓ **Установить режим работы «Открыто».** Приводит к разблокировке исполнительного устройства (ИУ) выбранного контроллера. ИУ остаются разблокированными в течение всего времени, пока данный режим не будет изменен. Нажатие на кнопки ДУ исполнительным устройством игнорируются. При предъявлении карт доступа к считывателям данного контроллера регистрируются события о проходе или нарушении доступа. При этом фиксируются причины нарушения в зависимости от прав доступа предъявленной карты.
- ✓ **Установить режим работы «Контроль».** Приводит к блокировке ИУ выбранного контроллера. При нажатии на кнопку ПУ для данного направления или при поднесении карты, удовлетворяющей всем критериям разрешения доступа в данном направлении, данное направление ИУ разблокируется на время равное времени удержания данного направления ИУ в открытом состоянии. Последующая блокировка данного направления ИУ происходит либо после прохода в данном направлении; либо по истечению времени удержания данного направления ИУ в открытом состоянии.

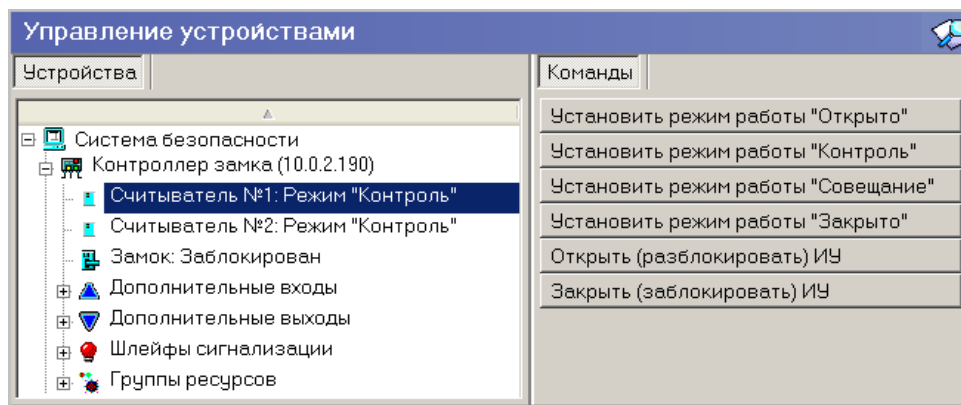
- ✓ **Установить режим работы «Совещание».** Аналогично режиму работы «Контроль» За исключением индикации на считывателях и блоке внутренней индикации. Более подробно об индикации режимов работы изложено в техническом описании системы безопасности.
- ✓ **Установить режим работы «Закрото».** Приводит к разблокировке исполнительного устройства (ИУ) выбранного контроллера. ИУ остаются заблокированными в течение всего времени, пока данный режим не будет изменен. Нажатие на кнопку ДУ исполнительным устройством игнорируется. Предъявление любой карты вызывает регистрацию события о нарушении прав доступа. Проход через ИУ (открытый механически) вызывает регистрацию события о несанкционированном проходе через ИУ и, при задании соответствующих опций, включение сигнала тревоги.
- ✓ **Открыть (разблокировать) ИУ.** Приводит к разблокировке ИУ выбранного контроллера на указанное время .
- ✓ **Закреть (заблокировать) ИУ.** Приводит к блокировке ИУ выбранного контроллера на указанное время
- ✓ **Поднять тревогу.** Приводит к запуску выбранным контроллером механизма реакции на возникновение тревожной ситуации. Параметры обработки тревожной ситуации для выбранного контроллера описываются в «[Генераторе тревоги](#)».
- ✓ **Сбросить тревогу.** Приводит к прекращению выполнения выбранным контроллером механизма обработки тревожной ситуации.
- ✓ **Активизировать дополнительные выходы.** Приводит к активизации всех дополнительных выходов выбранного контроллера.
- ✓ **Нормализовать дополнительные выходы.** Приводит к нормализации всех дополнительных выходов выбранного контроллера.
- ✓ **Сбросить зональность идентификаторов.** Приводит к сбросу зональности всех идентификаторов, связанных с выбранным контроллером. Эта команда тесно связана с параметром ИУ «[Внутренняя защита от передачи идентификаторов](#)», и имеет смысл, если этот параметр задействован. После выполнения данной команды всем идентификаторам будет присвоена зона 0.
- ✓ **Получить состояние.** Выводит на экран отчет о состоянии контроллера на момент выполнения команды.



ПРИМЕЧАНИЕ

Невозможно воспользоваться командами «Открыть (разблокировать) ИУ» и «Закреть (заблокировать) ИУ» при установленных режимах работы «Открыто» и «Закрото».

Считыватель



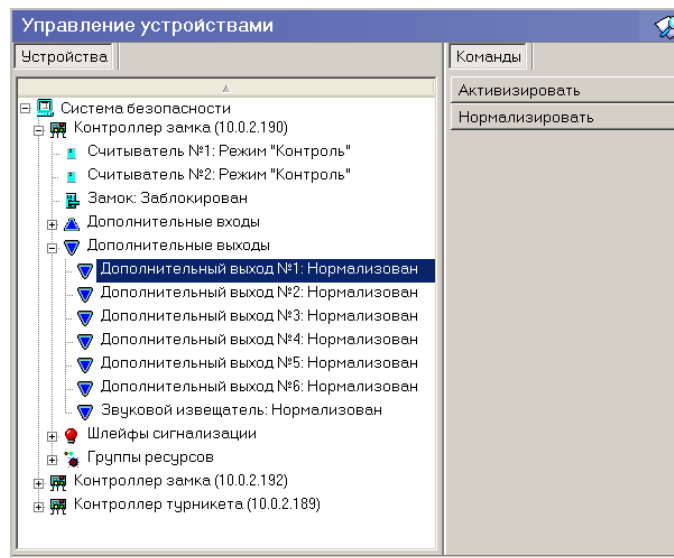
- ✓ **Установить режим работы «Открыто».** Приводит к разблокировке ИУ, связанного с выбранным считывателем. Исполнительное устройство остается разблокированным в течение всего времени пока данный режим не будет изменен. Нажатие на кнопки ДУ исполнительным устройством игнорируется. При поднесении карты доступа к считывателю регистрируется событие о проходе или нарушении доступа. При этом фиксируются причины нарушения в зависимости от прав доступа предъявленной карты.
- ✓ **Установить режим работы «Контроль».** Приводит к блокировке ИУ, связанного с выбранным считывателем. При нажатии на кнопку ДУ для данного направления или при поднесении карты, удовлетворяющей всем критериям разрешения доступа в данном направлении, данное направление ИУ разблокируется на время, которое равно времени удержания данного направления ИУ в открытом состоянии. Последующая блокировка данного направления ИУ происходит либо после прохода в данном направлении; либо по истечению времени удержания данного направления ИУ в открытом состоянии.
- ✓ **Установить режим работы «Совещание».** Аналогично режиму доступа «Контроль» за исключением индикации на считывателе и блоке внутренней индикации. Более подробно об индикации режимов доступа изложено в техническом описании системы безопасности.
- ✓ **Установить режим работы «Закрото».** При включении режима данное направление ИУ блокируется и остается заблокированным в течение всего времени пока режим включен. Нажатие на кнопку ДУ для данного направления игнорируется. Предъявление любой карты вызывает регистрацию события о нарушении прав доступа. Проход через ИУ (открытый механически) вызывает регистрацию события о несанкционированном проходе через ИУ и, при задании соответствующих опций, включение сигнала тревоги.
- ✓ **Открыть (разблокировать) ИУ.** Приводит к разблокировке выбранного считывателя на указанное время.
- ✓ **Закреть (заблокировать) ИУ.** Приводит к блокировке выбранного считывателя на указанное время.



ПРИМЕЧАНИЕ

Невозможно воспользоваться командами «Открыть (разблокировать) ИУ» и «Закреть (заблокировать) ИУ» при установленных режимах работы «Открыто» и «Закрото».

Дополнительный выход



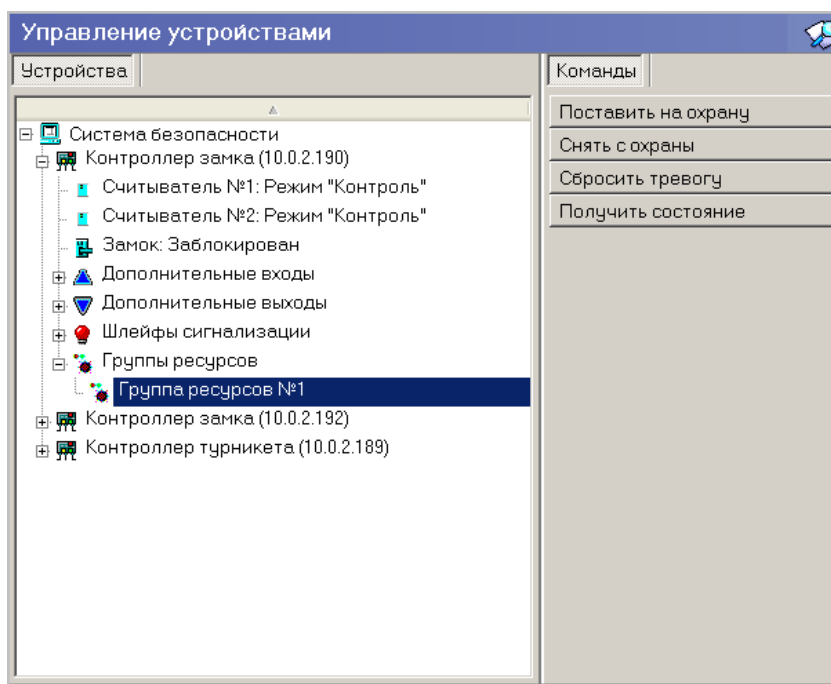
- ✓ **Активизировать.** Приводит к переводу выбранного дополнительного выхода в активное состояние.
- ✓ **Нормализовать.** Приводит к переводу выбранного дополнительного выхода в нормальное состояние.



ПРИМЕЧАНИЕ

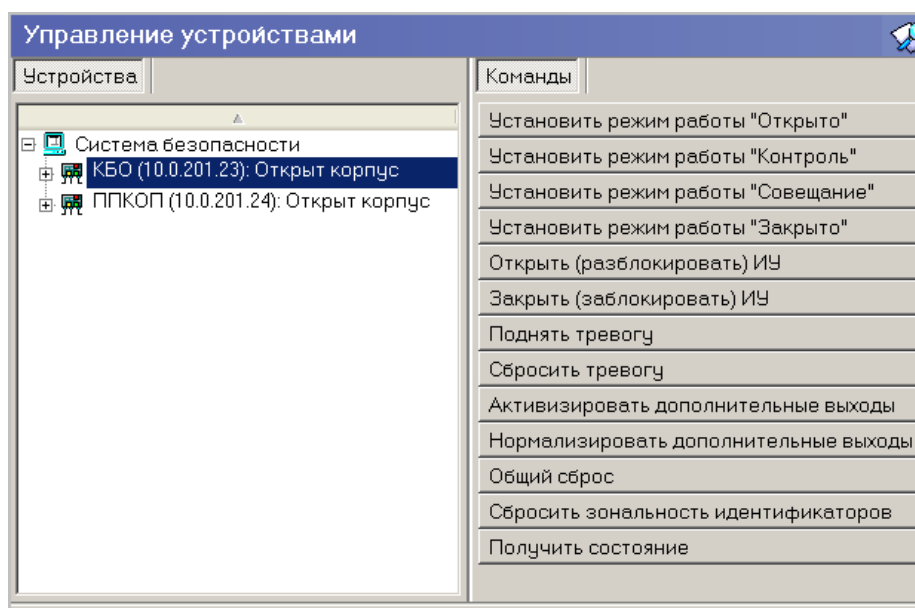
Если тип дополнительного выхода описан как ОПС или генератора тревоги, то попытка активировать или нормализовать этот выход приведет к ошибке – «Несоответствие типа ресурса».

Группа ресурсов



- ✓ **Поставить на охрану.** Приводит к постановке выбранной группы ресурсов на охрану. Если в состав выбранной группы ресурсов входит исполнительное устройство (ИУ), то оно блокируется и остается заблокированным в течение всего времени пока режим включен. Нажатие на кнопку ДУ игнорируется. Открывание двери в режиме постановки на охрану вызывает регистрацию события о несанкционированном проходе через ИУ и, при задании соответствующих опций, включение сигнала тревоги. Если по истечении времени выдачи сигнала тревоги дверь будет закрыта (вход Pass нормализуется), сигнал тревоги выключается. Иначе выдача сигнала тревоги продолжается до закрытия двери. Если в выбранную группу ресурсов входит шлейф охранной сигнализации, то ШС переходит в состояние «на охране». Если сопротивление ШС, устанавливаемого на охрану, не в норме, ШС переходит в состояние «не взятие» через время задержки, задаваемое при конфигурации. Для взятого на охрану ШС контроллер отслеживает сопротивление в его линии и принимает решение о его состоянии.
- ✓ **Снять с охраны.** Происходит снятие группы ресурсов с охраны. Если в состав группы ресурсов входит ИУ, то контроллер переходит в режим работы «Контроль». Если в состав группы ресурсов входит шлейф сигнализации, контроллер перестает отслеживать сопротивление в его линии.
- ✓ **Сбросить тревогу.** Приводит к сбросу тревоги и прекращению выполнения алгоритма обработки тревожной ситуации.
- ✓ **Получить состояние.** Выводит на экран отчет о состоянии группы ресурсов на момент выполнения команды.

Контроллер КБО

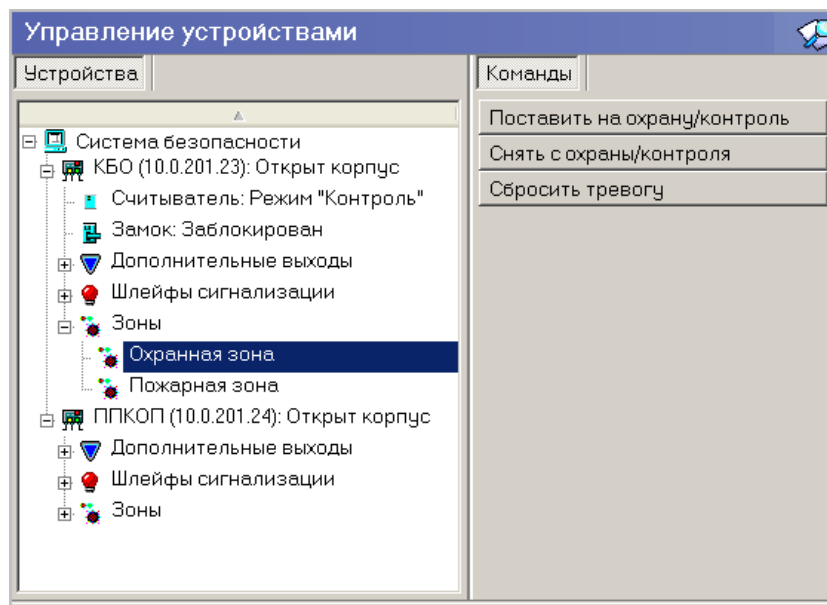


- ✓ **Установить режим работы «Открыто».** Приводит к разблокировке исполнительного устройства (ИУ) выбранного контроллера. ИУ остаются разблокированными в течение всего времени, пока данный режим не будет изменен. Нажатие на кнопки ДУ исполнительным устройством игнорируются. При предъявлении карт доступа к считывателям данного контроллера регистрируются события о проходе или нарушении доступа. При этом фиксируются причины нарушения в зависимости от прав доступа предъявленной карты.
- ✓ **Установить режим работы «Контроль».** Приводит к блокировке ИУ выбранного контроллера. При нажатии на кнопку ПУ для данного направления или при

поднесении карты, удовлетворяющей всем критериям разрешения доступа в данном направлении, данное направление ИУ разблокируется на время равное времени удержания данного направления ИУ в открытом состоянии. Последующая блокировка данного направления ИУ происходит либо после прохода в данном направлении; либо по истечению времени удержания данного направления ИУ в открытом состоянии.

- ✓ **Установить режим работы «Совещание».** Аналогично режиму работы «Контроль» За исключением индикации на считывателях и блоке внутренней индикации. Более подробно об индикации режимов работы изложено в техническом описании системы безопасности.
- ✓ **Установить режим работы «Закрыто».** Приводит к разблокировке исполнительного устройства (ИУ) выбранного контроллера. ИУ остаются заблокированными в течение всего времени, пока данный режим не будет изменен. Нажатие на кнопку ДУ исполнительным устройством игнорируется. Предъявление любой карты вызывает регистрацию события о нарушении прав доступа. Проход через ИУ (открытый механически) вызывает регистрацию события о несанкционированном проходе через ИУ и, при задании соответствующих опций, включение сигнала тревоги.
- ✓ **Открыть (разблокировать) ИУ.** Приводит к разблокировке ИУ выбранного контроллера на указанное время .
- ✓ **Закрыть (заблокировать) ИУ.** Приводит к блокировке ИУ выбранного контроллера на указанное время
- ✓ **Поднять тревогу.** Приводит к запуску выбранным контроллером механизма реакции на возникновение тревожной ситуации. Параметры обработки тревожной ситуации для выбранного контроллера описываются в «[Генераторе тревоги](#)».
- ✓ **Сбросить тревогу.** Приводит к прекращению выполнения выбранным контроллером механизма обработки тревожной ситуации.
- ✓ **Активизировать дополнительные выходы.** Приводит к активизации всех дополнительных выходов выбранного контроллера.
- ✓ **Нормализовать дополнительные выходы.** Приводит к нормализации всех дополнительных выходов выбранного контроллера.
- ✓ **Сбросить зональность идентификаторов.** Приводит к сбросу зональности всех идентификаторов, связанных с выбранным контроллером. Эта команда тесно связана с параметром ИУ «[Внутренняя защита от передачи идентификаторов](#)», и имеет смысл, если этот параметр задействован. После выполнения данной команды всем идентификаторам будет присвоена зона 0.
- ✓ **Общий сброс.** Приводит к сбросу контроллера при котором состояния всех ШС инициализируются, с ПШС снимается питание на время *Задержка сброса ПШС*, у ОЗ снимается тревога.
- ✓ **Получить состояние.** Выводит на экран отчет о состоянии ресурсов контроллера на момент выполнения команды.

Зона контроллера КБО



- ✓ **Поставить на охрану/контроль.** Приводит к постановке выбранной зоны на охрану/контроль. Если в состав выбранной зоны входит исполнительное устройство (только для КБО), то оно блокируется и остается заблокированным в течение всего времени пока режим включен. Нажатие на кнопку ДУ игнорируется. Открывание двери в режиме постановки на охрану вызывает регистрацию события о несанкционированном проходе через ИУ и, при задании соответствующих опций, включение сигнала тревоги. Если по истечении времени выдачи сигнала тревоги дверь будет закрыта (вход Pass нормализуется), сигнал тревоги выключается. Иначе выдача сигнала тревоги продолжается до закрытия двери. Если в выбранную зону входит шлейф сигнализации, то ШС переходит в состояние «на охране». Если сопротивление ШС, устанавливаемого на охрану, не в норме, ШС переходит в состояние «не взятие» через время задержки, задаваемое при конфигурации. Для взятого на охрану ШС контроллер отслеживает сопротивление в его линии и принимает решение о его состоянии.
- ✓ **Снять с охраны/контроля.** Происходит снятие зоны с охраны/контроля. Если в состав зоны входит ИУ, то контроллер переходит в режим работы «Контроль». Если в состав зоны входит шлейф сигнализации, контроллер перестает отслеживать сопротивление в его линии.
- ✓ **Сбросить тревогу.** Приводит к сбросу тревоги и прекращению выполнения алгоритма обработки тревожной ситуации.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Инсталляция
Лицензия
Контроллер
Сетевые настройки
Адрес
ДНСР
Конфигурация
Параметры контроллеров
Тестовый вход
Релейный выход
Исполнительное устройство
Считыватель
Тревога
Генератор тревоги
Шлейф сигнализации
Группа ресурсов
Защита от передачи идентификаторов
Сотрудник
Доступ
Параметры доступа
Управление устройствами
Сервер
База данных
Резервная копия БД
Оптимизация индексов БД
Пароль
Проход
Аппаратура
Событие
Команды управления