ОАО «Бауманн»

УТВЕРЖДЕН
RU.74533456.00021-02 34 01-ЛУ

Интегрированный комплекс безопасности «КОДОС»

Руководство администратора

RU.74533456.00021-02 34 01

2015

SEC.RU | Короткий путь к информации
Скачано с sec.ru

СОДЕРЖАНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ 4
1.1 Назначение 4
1.2 Условия выполнения программы 4
2 УСТАНОВКА ПРОГРАММЫ 5
2.1 Подготовка к установке 5
2.2 Установка программы 5
2.3 Настройка подключения к базе данных 9
2.4 Окончание установки 11
2.5 Защита ПО «КОДОС» от несанкционированного использования 12
2.6 Удаление программы 14
2.7 Обновление программы 15
2.7.1 Настройки в программе «Конфигуратор» 15
3 НАСТРОЙКИ В ИКБ «КОДОС» 16
3.1 Вход в программу 16
3.2 Настройка системы 16
3.2.1 Вкладка «Основные параметры» 17
3.2.2 Вкладка «Технические параметры» 19
3.3 Создание списка операторов 20
3.4 Назначение прав операторам 22
3.5 Настройка модуля «Владельцы» 26
3.6 Добавление АРМ 29
3.7 Настройка АРМ 31
3.7.1 Вкладка «Локальные параметры» 31
3.7.2 Вкладка «Технические параметры» 33
3.8 Настройка временных зон 34
3.9 Настройка праздников 35
3.10 Настройка групп датчиков 36
3.11 Настройка групп дверей 38
3.12 Настройка звуков 41
3.13 Настройка правил 42
3.14 Настройка видеозаписи 46
3.15 Настройка интегрированного видео 50
3.16 Управление поворотным устройством 51
3.17 Мультиконфигурации 58
3.18 Настройка режима запрета повторного прохода 65
3.18.1 Настройка глобального ЗПП 65
3.18.2 Настройка локального ЗПП 66
3.19 Настройка режима контроля оператора 67
3.20 Настройка фильтра отображаемых событий 68
3.21 Настройка функции контроля обхода охранника 69
3.22 Настройка свойств двери 71

SEC.RU | Короткий путь к информации Скачано с sec.ru

3.23 Настройка «Кабинетного режима» ... 72
3.23.1 Изменение режима работы контроллера с помощью ПО ИКБ «КОДОС» ... 73
3.23.2 Управление режимами контроллеров серии «КОДОС ЕС-ХХХ М» с помощью карты доступа ... 73
3.24 Настройка исполнительного устройства для «КОДОС ЕС-202 М» и «КОДОС ЕС-304 М» ... 77
3.25 Особенности настройки контроллера шлюза ... 78
3.26 Настройка картоприемника ... 79
3.27 Планировщик задач ... 81
3.28 Настройка функции отложенного опроса панелей «А-20» ... 81
4 ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ ПРОГРАММЫ ... 82
4.1 Установка и настройка USB-считывателя ... 82
4.2 Настройка модуля «Персонализации карт» ... 85
4.3 Настройка модуля «Учет и выдача карт посетителям» ... 86
4.4 Настройка модуля «Дизайн пропусков» ... 87
5 УСТАНОВКА КЛИЕНТСКИХ РАБОЧИХ МЕСТ ... 88
6 КОНФИГУРИРОВАНИЕ ИКБ «КОДОС» ДЛЯ КРУПНЫХ ОБЪЕКТОВ ... 89
6.1 Настройка контроллеров с помощью утилиты ContrTools ... 89
6.2 Использование локальных индексов ... 89
6.2.1 Пример настройки ... 90
7 РАБОТА И ОБСЛУЖИВАНИЕ ПРОГРАММЫ ... 91
7.1 Логика обработки прохода пользователя ... 91
7.1.1 Настройка прохода пользователя ... 93
7.2 Обслуживание базы данных ... 94
7.2.1 Выгрузка событий из БД ... 94
7.2.2 Проверка, копирование и восстановление БД ... 96
8 ПРИЛОЖЕНИЕ «А». Глоссарий ... 97

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Интегрированный комплекс безопасности (ИКБ) «КОДОС» включает в себя системы контроля и управления доступом, охранно-пожарной сигнализации, определения номеров автотранспорта, видеонаблюдения и жизнеобеспечения объекта, объединенные общей информационной средой.

Предполагается, что персонал, проводящий настройку оборудования, обладает не только базовыми навыками работы с ПК и основными понятиями о системах контроля доступа (СКД), охранно-пожарной (ОПС) и системах видеонаблюдения, но также имеет представление об основных принципах построения локальной сети, обладает навыками установки и настройки оборудования и конфигурирования программного обеспечения.

Это руководство может также быть использовано для обучения работе с программным обеспечением ИКБ «КОДОС».

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение

ИКБ — это система комплексного управления безопасностью объекта. Комплекс «КОДОС» даёт возможность оператору системы безопасности получать полную, достоверную и оперативную информацию о состоянии безопасности на объекте.

Руководство предназначено для инженеров монтажных организаций, системных администраторов, сотрудников IT-отделов организаций, занимающихся установкой, настройкой и обслуживанием ИКБ «КОДОС». Руководство содержит полные сведения, необходимые для правильной инсталляции и использования возможностей системы.

1.2 Условия выполнения программы

1. Рекомендуемые требования к программному обеспечению компьютера:

- Windows 7.
- Файловая система NTFS.
- Программы Microsoft Word, Excel из пакета MS Office (для работы с отчетами).

2. Минимальные требования к компьютеру при работе ИКБ «КОДОС» (без видеонаблюдения):

- Двухъядерный процессор с тактовой частотой 2гГц.
- Объем оперативной памяти (ОЗУ) – 2ГБ.
- Объем жесткого диска – 250 ГБ.

3. Рекомендуемые требования к компьютеру при работе ИКБ «КОДОС» (без видеонаблюдения):

- Многоядерный процессор с тактовой частотой от 3 гГц.
- Объем оперативной памяти (ОЗУ) – 4 ГБ.
- Объем жесткого диска –1ТБ.

Рекомендуемые требования к компьютеру при работе ИКБ «КОДОС» с программой «GLOBOSS» зависят от количества видеоканалов.

Количество видеоканалов				
	До 4	До 8	До 16	Свыше 16
Процессор	Intel Core i3-4330 3.5 GHz	Intel Core i5-4430 3.2 GHz	Intel Core i7-4770 3.9 GHz	Intel Core i7-4770 3.9 GHz
Жесткий диск	1ТБ	1ТБ	2ТБ	2ТБ
Оперативная память, Мб	4096 (2x2048)	4096 (2x2048)	8192 (2x4096)	8192 (2x4096)
Видеокарта	AMD Redeon R7 240 nVidia GT 730 (128-bit)	AMD Redeon R7 240 nVidia GT 730 (128-bit)	AMD Redeon R7 240 nVidia GT 730 (128-bit)	AMD Redeon R7 240 nVidia GT 730 (128-bit)

ВНИМАНИЕ! Выбор объема жесткого диска определяется количеством камер видеонаблюдения и параметрами записи.

- Требования установлены по состоянию на март 2015 года и могут быть изменены.
- При обновлении ПО с более ранних версий возможна его работа на существующей конфигурации оборудования.
- Не рекомендуется использовать на одном ПК ПО ИКБ «КОДОС» совместно с программой «GLOBOSS» при количестве каналов больше 16 из-за большой загрузки процессора. В этом случае программу «GLOBOSS» необходимо устанавливать на отдельный ПК.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2 УСТАНОВКА ПРОГРАММЫ

2.1 Подготовка к установке

ВНИМАНИЕ! Инсталлировать систему необходимо под профилем «Администратор», устанавливаемого ОС Windows по умолчанию.

Если в конфигурации задействовано оборудование, использующее COM-порт, например, сетевой контроллер КОДОС СК–232 или ППКОП А-20, необходимо выполнить команду: «Пуск» → «Панель управления» → «Система» → «Диспетчер устройств» → «Порты (COM и LPT)» → «Последовательный порт (COM1)» (Свойства) → «Параметры порта» → «Дополнительно».

В окне «Дополнительные параметры COM1» снять флаг «Использовать буферы FIFO» (Рисунок 2.1).

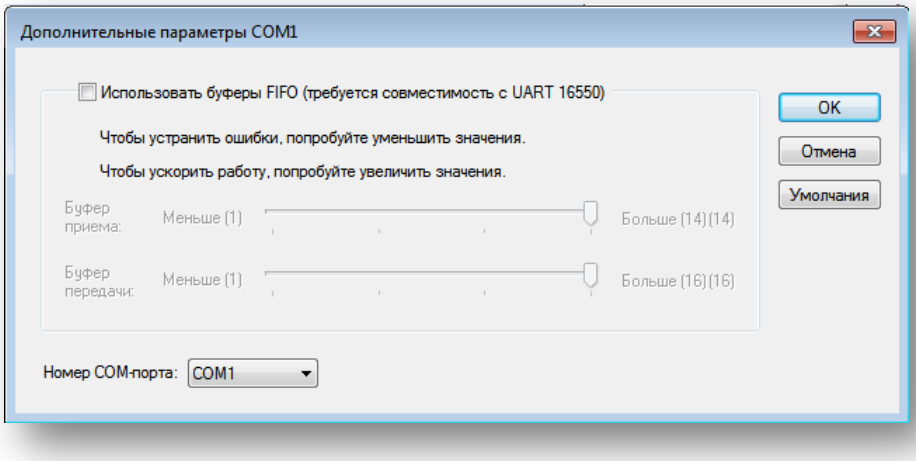


Рисунок 2.1

2.2 Установка программы

Установка ИКБ «КОДОС» выполняется с помощью программы инсталлятора.

- Запустите на исполнение файл setup.exe и следуйте указаниям мастера установки. Программа предложит выбрать язык (см. рисунок ниже):

SEC.RU | Короткий путь к информации Скачано с sec.ru

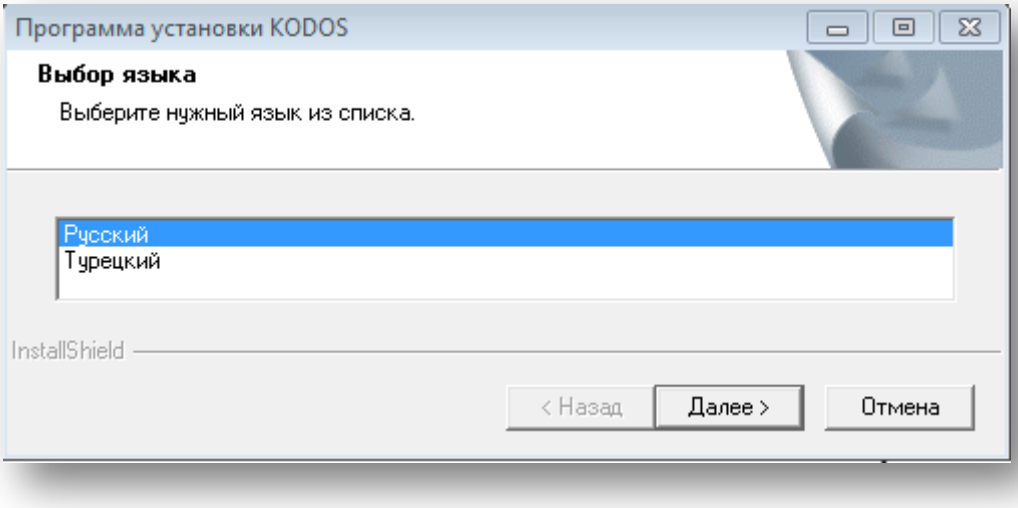


Рисунок 2.2

- Установка и использование программы возможна только при согласии с условиями лицензионного соглашения.
- Устанавливаемый комплект ПО ИКБ «КОДОС» содержит в себе сервер СУБД Firebird v. 2.5.2

(Рисунок 2.3).

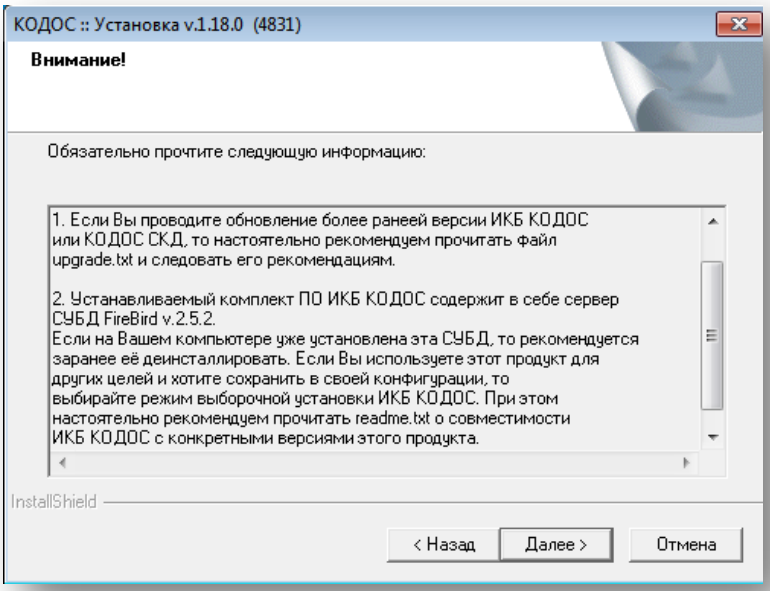


Рисунок 2.3

- В окне «Выбор папки назначения» укажите папку, в которую будут установлены файлы (Рисунок 2.4).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

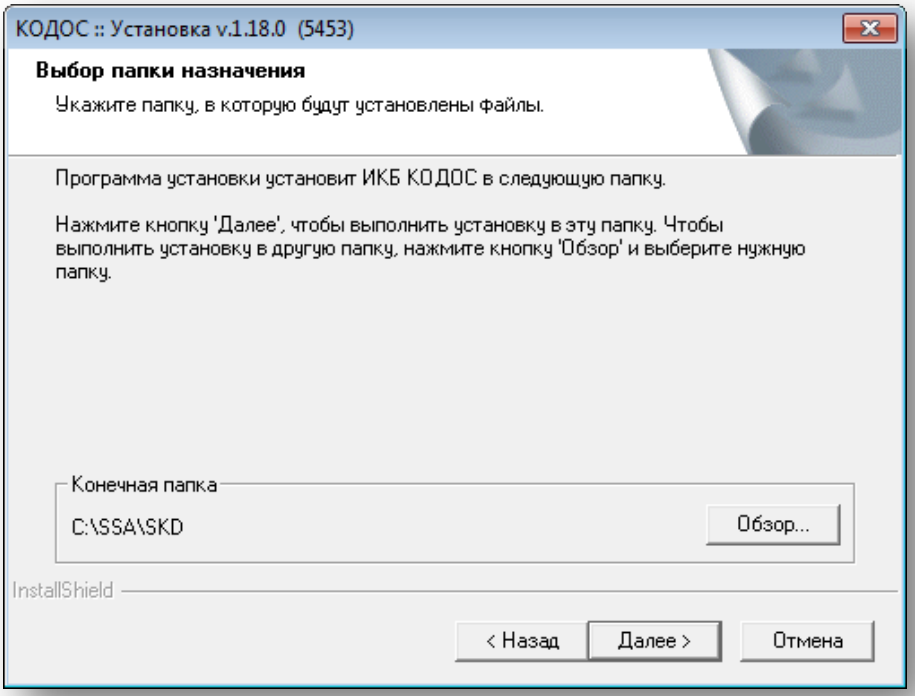


Рисунок 2.4

- Укажите вид установки (Рисунок 2.5). Рекомендуется воспользоваться готовыми шаблонами установки. Если Вы опытный пользователь, можете использовать вид установки «Специальный» и самостоятельно выбирать устанавливаемые компоненты.

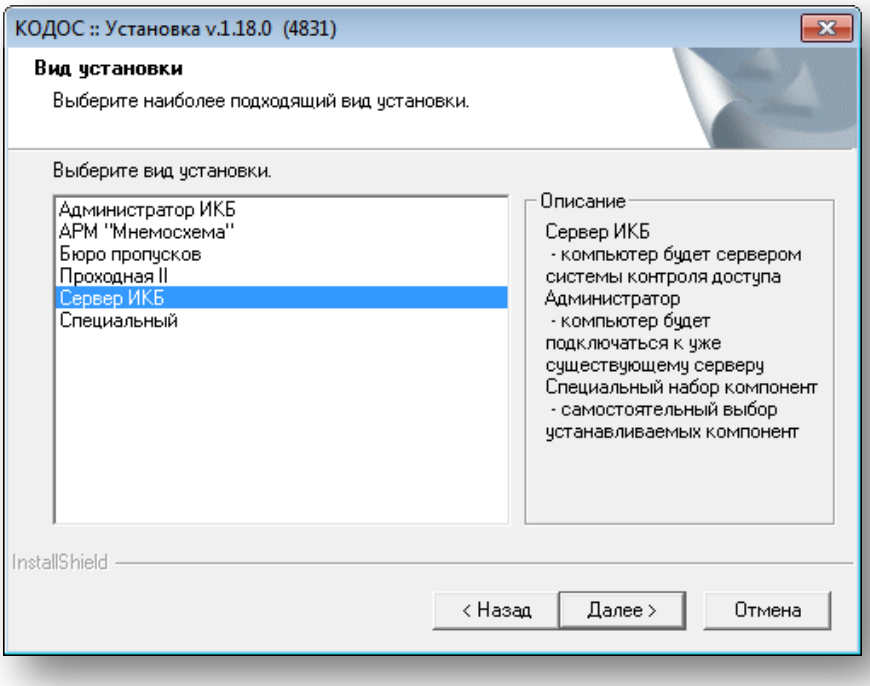


Рисунок 2.5

- При выборе компонентов ИКБ (Рисунок 2.6) руководствуйтесь наличием лицензии на устанавливаемые модули. Без лицензии установленный модуль будет недоступен.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

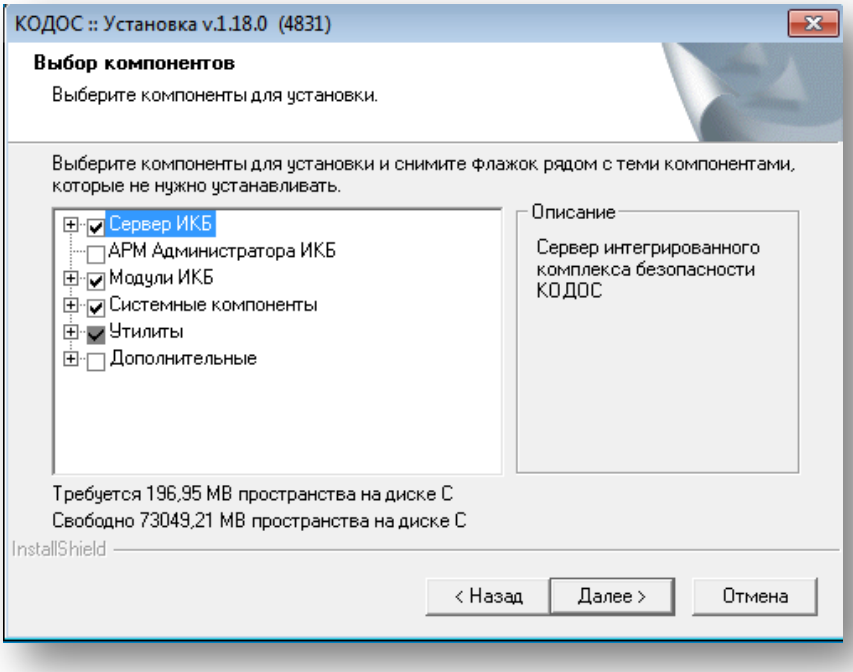


Рисунок 2.6

- Далее укажите (или выберите из списка) папку, в которую программа добавит значки (Рисунок 2.7).

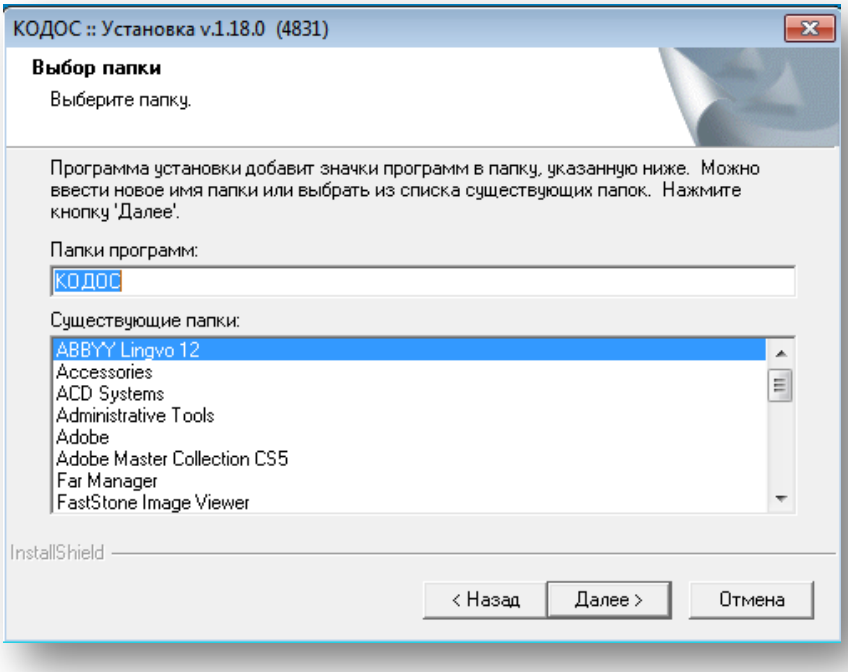


Рисунок 2.7

- При интеграции ИКБ «КОДОС» с системой видеонаблюдения необходимо, в зависимости от того, какая именно система («КОДОС-ВИДЕОСЕТЬ» или «GLOBOSS») будет использоваться, выбрать соответствующий компонент. Одновременное использование обеих систем не допускается. Так же следует поступить с компонентами «Бюро пропусков» и «Учет карт посетителей» — одновременное использование невозможно.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.3 Настройка подключения к базе данных

Для правильного обращения программ ИКБ «КОДОС» к базе данных (БД) необходимо правильно настроить используемые конфигурации базы данных.

- Запустите настройку базы данных: «Пуск» → «Все программы» → ИКБ «КОДОС» → «Утилиты» → «Настройка баз данных». Откроется окно «Выбор рабочей БД» (Рисунок 2.8).

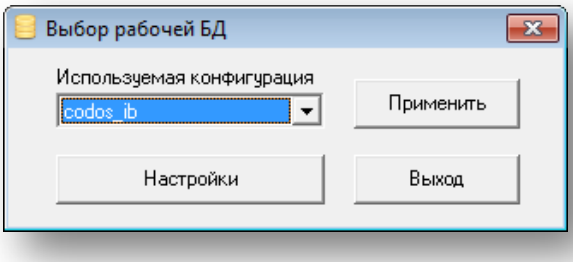


Рисунок 2.8

При установке «Сервер ИКБ» и СУБД FireBird с инсталляционного диска, псевдоним СУБД уже настроен, имеет имя «codos_ib».

- Нажмите кнопку «Настройки». В окне «Настройка подключения к базам данных» (Рисунок 2.9) в левой части окна необходимо, исходя из имеющихся СУБД, создать конфигурацию подключения к БД, в правой — следует указать параметры ее подключения.

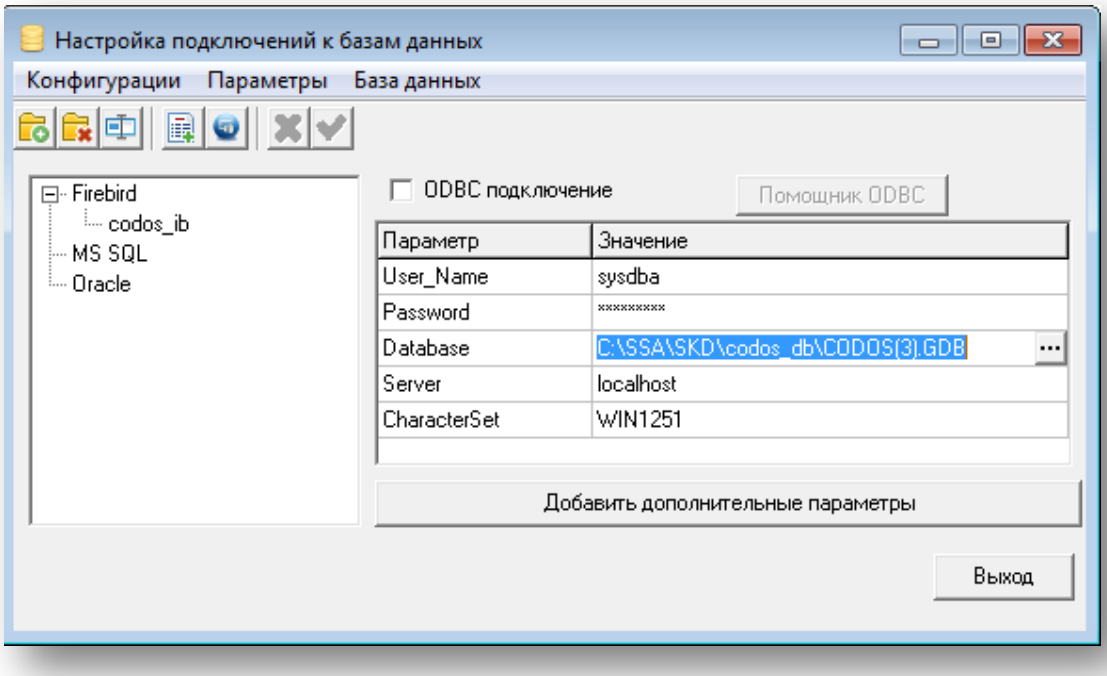


Рисунок 2.9

- В строке «User_Name» введите имя учетной записи в БД.
- В строке «Password» — введите пароль учетной записи в БД.

При установке системы ИКБ «КОДОС» с БД Firebird по умолчанию определены: имя — «sysdba», пароль — «masterkey».

- В строке «Database» укажите путь к базе данных. Кнопка ... станет активной при однократном щелчке левой кнопкой мыши в поле ввода.
- Если БД находится на Вашем компьютере, укажите путь к БД:

«Диск установки»: \ SSA \ SKD \ codos_db \ имя файла БД. В строке Server — localhost.

- Для настройки подключения с клиентского рабочего места к БД, расположенной на сервере, в строке Database укажите путь к БД на сервере:

SEC.RU | Короткий путь к информации Скачано с sec.ru

«Диск установки»: \ SSA \ SKD \ codos_db\ «имя файла БД». В строке Server введите IP-адрес или имя сервера. Опции главного меню продублированы кнопками на панели инструментов.

- Вы можете создать несколько конфигураций подключения к БД. Для добавления конфигурации щелкните кнопку . В списке конфигураций появится новая, вида: db_FB_1 .
- Для редактирования названия конфигурации нажмите кнопку .
- Кнопка удаляет выделенную конфигурацию.
- При необходимости вы можете указать индивидуальные значения параметров подключения для базы данных. Для этого нажмите кнопку или Добавить дополнительные параметры
- После настройки требуемых параметров важно проверить правильность введенных данных. Для проверки связи с базой данных нажмите . При успешном установлении связи появится сообщение:

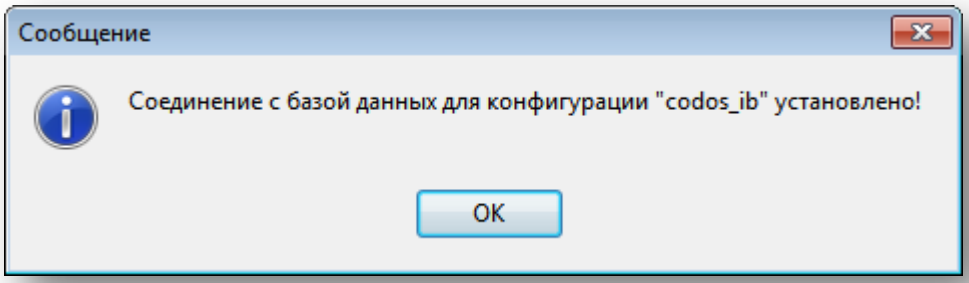


Рисунок 2.10

Если значения параметров заданы с ошибкой, при нажатии кнопки проверки связи с БД будет выведено сообщение:

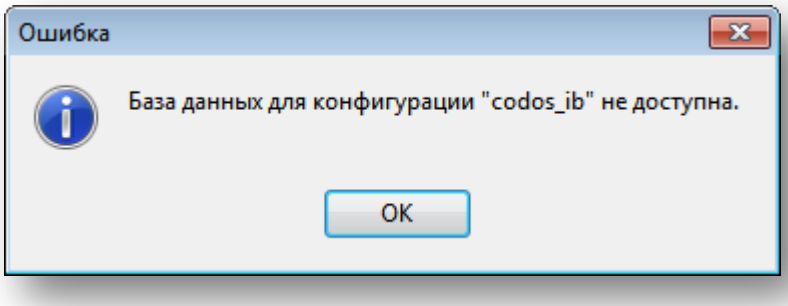


Рисунок 2.11

- Нажатие кнопки отменяет все внесенные изменения.
- Кнопка предназначена для сохранения настроек подключения к БД.

По завершении всех настроек нажмите кнопку «Выход».

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.4 Окончание установки

- Запустите программу «Конфигуратор»: «Пуск» → «Программы» → «ИКБ КОДОС» → «Конфигуратор» (Рисунок 2.12).

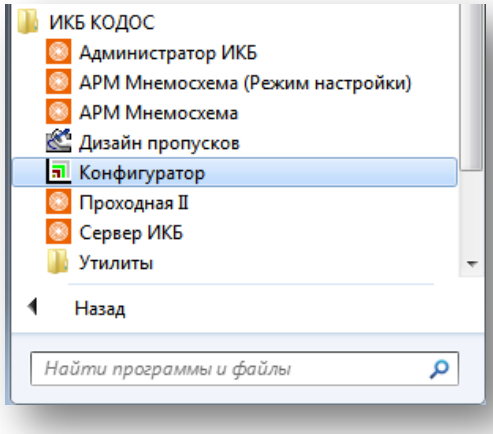


Рисунок 2.12

- В выпадающем списке выберите используемую конфигурацию для подключения к базе данных и нажмите кнопку «Выбрать» (Рисунок 2.13).

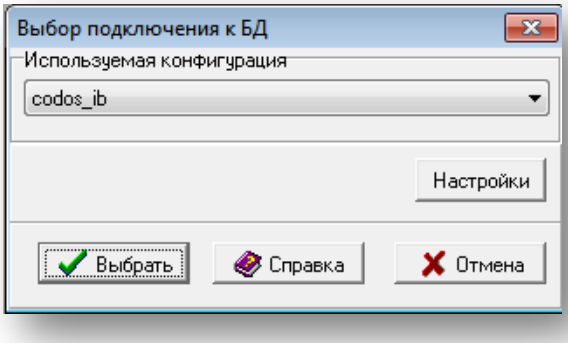


Рисунок 2.13

Для авторизации оператора системы ведите имя (ADMIN) и пароль (power).

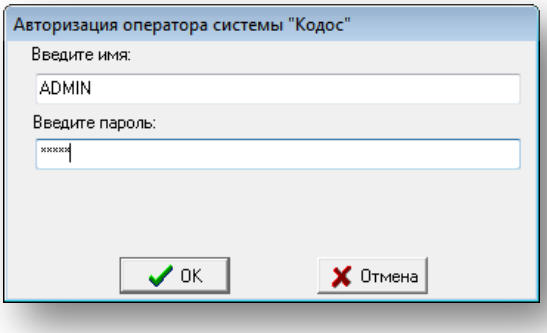


Рисунок 2.14

ВНИМАНИЕ! При обновлении программы с предыдущих версий возможно появление окна с предложением обновить базу данных. В этом случае необходимо согласиться — все необходимые изменения будут внесены автоматически.

- Закройте программу «Конфигуратор»
- Зарегистрируйте лицензионный ключ. Порядок ввода лицензионного ключа описан в п. Защита ПО «КОДОС» от несанкционированного использования.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2.5 Защита ПО «КОДОС» от несанкционированного использования

Программное обеспечение имеет защиту от несанкционированного использования. Она реализована в виде аппаратных и программных средств, препятствующих незаконному запуску и работе ПО. Пользователь, приобретая программный продукт торговой марки «КОДОС», получает ключ аппаратной защиты и лицензию.

ВНИМАНИЕ! Не предусмотрена эксплуатация ПО семейства «КОДОС» без ключа аппаратной защиты.

Ключ аппаратной защиты — техническое средство защиты на аппаратном уровне от несанкционированного копирования и эксплуатации ПО. Совместно с лицензией ключ позволяет использовать программные модули для обеспечения работы подключенного оборудования.

Ключ аппаратной защиты — это USB-ключ, который во время работы с ПО «КОДОС» постоянно должен находиться в USB-разъеме. ИКБ может работать с несколькими ключами защиты

ВНИМАНИЕ! В новых версиях ПО сохранена поддержка LPT-ключей защиты.

При изъятии ключа защиты или отсутствии лицензии на использование программного обеспечения появляется окно с предупреждением о прекращении работы программы.

Установка драйверов для ключей защиты выполняется в автоматическом режиме при первой установке ключа после установки программы.

Лицензия на программный продукт даёт право на использование тех или иных компонентов «КОДОС» (программных модулей, режимов работы системы, количество подключаемого оборудования и т. д.) с конкретным ключом защиты и представляет собой текстовую строку специального вида: «XXXXXXXX-XXXXXXXX-...».

Лицензиями управляет специальная программа «Менеджер лицензий». Она устанавливается автоматически вместе с ПО. Запустить программу можно стандартным способом, например: Пуск → Программы (Все программы) → ИКБ «КОДОС» → Утилиты → Менеджер лицензий (Рисунок 2.15).

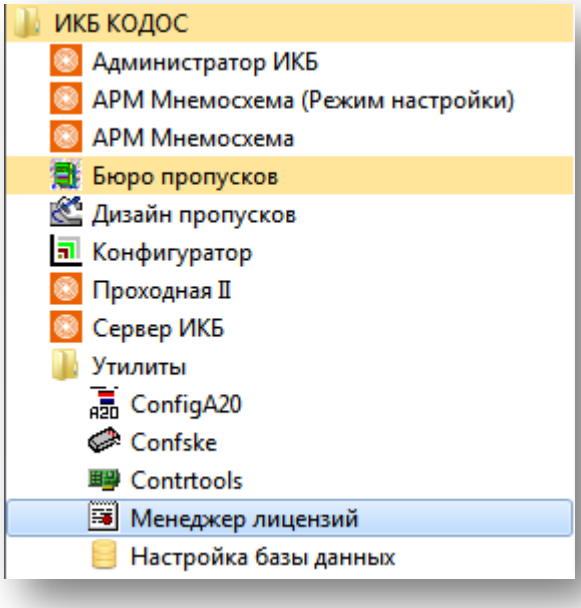


Рисунок 2.15

Главное окно программы представлено на рисунке ниже.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

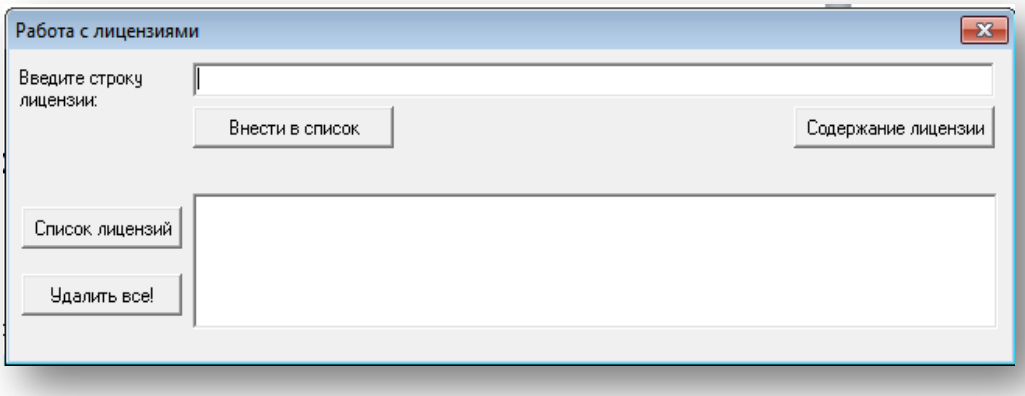


Рисунок 2.16

Код лицензии необходимо внести в поле «Введите строку лицензии». При наборе символов будьте внимательны, вводите только те символы, что указаны в лицензии. После проверки правильности ввода нажмите кнопку «Внести в список» (Рисунок 2.16).

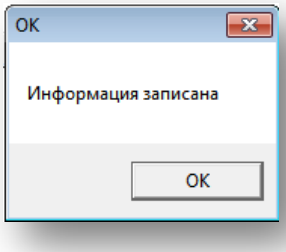


Рисунок 2.17

Появится сообщение о вводе (Рисунок 2.17), а в списке лицензий добавится введенный код (Рисунок 2.18).

Если в процессе эксплуатации программного продукта возникла необходимость расширения возможностей ПО (установка дополнительных модулей, увеличение числа используемого оборудования) или установки на один ПК нескольких программных продуктов, то необходимо добавить полученный код лицензии к уже имеющемуся (Рисунок 2.18).

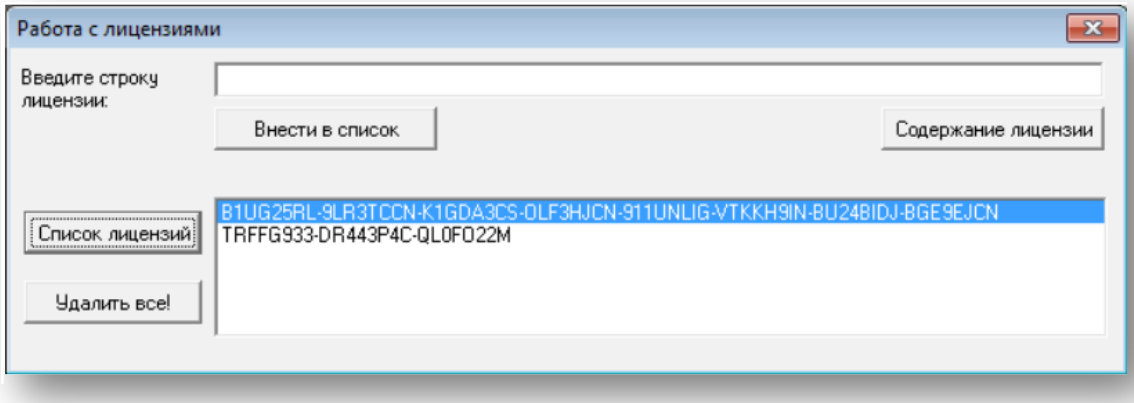


Рисунок 2.18

ПРИМЕЧАНИЕ – При необходимости расширения возможностей ПО, следует обратиться в ОАО «Бауманн» или представителям компании в регионах для переоформления лицензии. При использовании нескольких программных продуктов на одном ПК необходимо уточнить их совместимость у специалистов.

Содержание введенной лицензии можно узнать, нажав кнопку «Содержание лицензии»(Рисунок 2.16).

По завершении регистрации соответствующие ключу модули становятся доступными для использования.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.6 Удаление программы

ПРИМЕЧАНИЕ – Перед удалением программы рекомендуем сохранить базу данных ИКБ «КОДОС» в другом каталоге.

- Деинсталляцию рекомендуется выполнять стандартными средствами MS Windows, например, с помощью модуля «Установки и удаления программ» (команда Пуск=> Панель управления=>Программы и компоненты) (Рисунок 2.19).

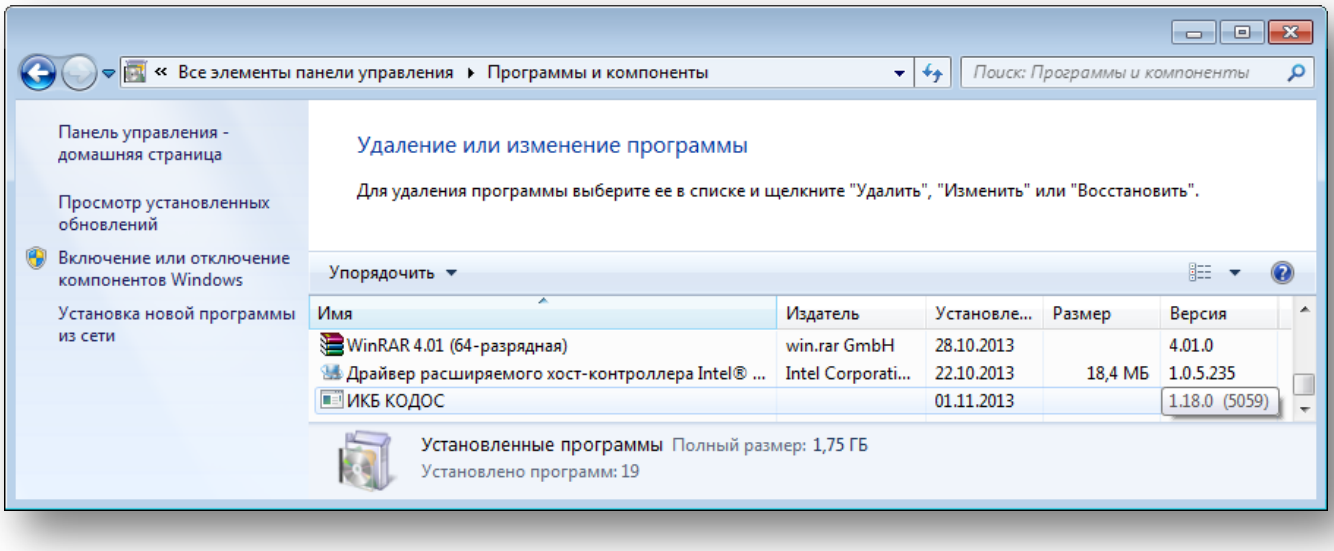


Рисунок 2.19

- В открывшемся окне (Рисунок 2.19) в разделе «Удаление и изменение программы» в предложенном списке выберите «ИКБ КОДОС» и нажмите кнопку «Удалить/ Заменить».
- ОС Windows вызовет программу «КОДОС::Установка» (Рисунок 2.20), в окне которой следует отметить «Удалить» и подтвердить нажатием кнопки «Далее>» — компьютер приступит к деинсталляции системы. По окончании процесса деинсталляции нажмите кнопку «Готово».

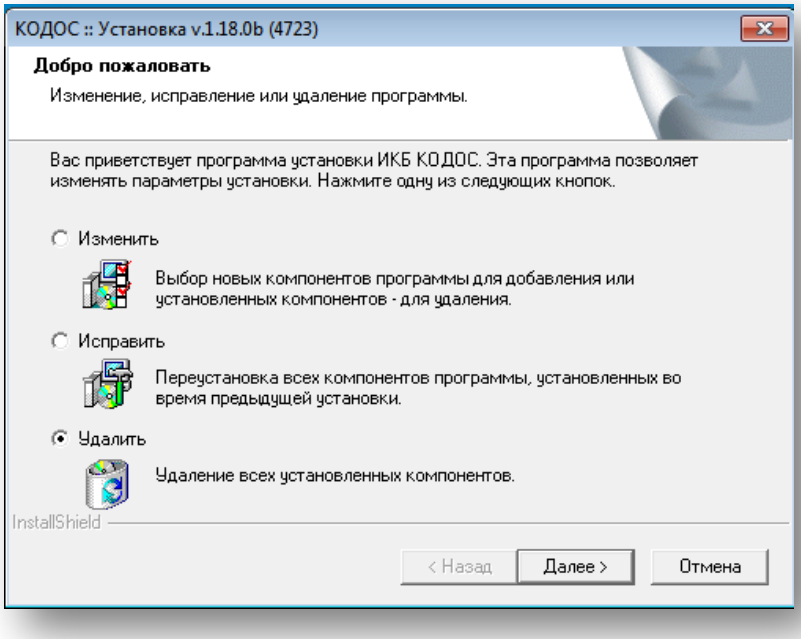


Рисунок 2.20

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.7 Обновление программы

ПРИМЕЧАНИЕ – Перед обновлением программы рекомендуется провести резервное копирование базы данных.

Для обновления версии программного обеспечения ИКБ «КОДОС» необходимо вначале деинсталлировать программу, как это указано в п. Удаление программы.

- Затем вставить установочный диск с новой версией ПО ИКБ «КОДОС» в CD-привод;
- Запустить на исполнение из папки Install файл setup.exe.
- Последовательно выполните действия, описанные в п. Установка программы.
- Чтобы не потерять данные из БД, после инсталляции новой версии ПО следует заменить файл с БД на сохраненный (см. примечание).

После окончания работы мастера установки необходимо запустить программу настройки системы («Конфигуратор»). При появлении предупреждения о необходимости конвертирования базы данных в новый формат нажмите «Да».

2.7.1 Настройки в программе «Конфигуратор»

«Конфигуратор» — программа, предназначенная для составления конфигурации подключенного оборудования ИКБ «КОДОС» и логической привязки этого оборудования к планам помещений.

«Конфигуратор» выполняет подготовительную настройку перед запуском управляющих программ ИКБ «КОДОС», например, программы «Сервер ИКБ» и «КОДОС-ОПС». Рекомендуется конфигурировать систему на том ПК, где планируется размещать сервер ИКБ.

ВНИМАНИЕ! Начиная с версии 1.16, не поддерживаются старые устройства (СК-А, СК-ЕС, Пульт А10, ЕС501, АБ А05), выпуск которых прекращен.

Подробнее о настройке системы см. «Руководство оператора программы „Конфигуратор“».

SEC.RU | Короткий путь к информации Скачано с sec.ru

3 НАСТРОЙКИ В ИКБ «КОДОС»

3.1 Вход в программу

- Запустите «Сервер ИКБ» (Рисунок 3.1).

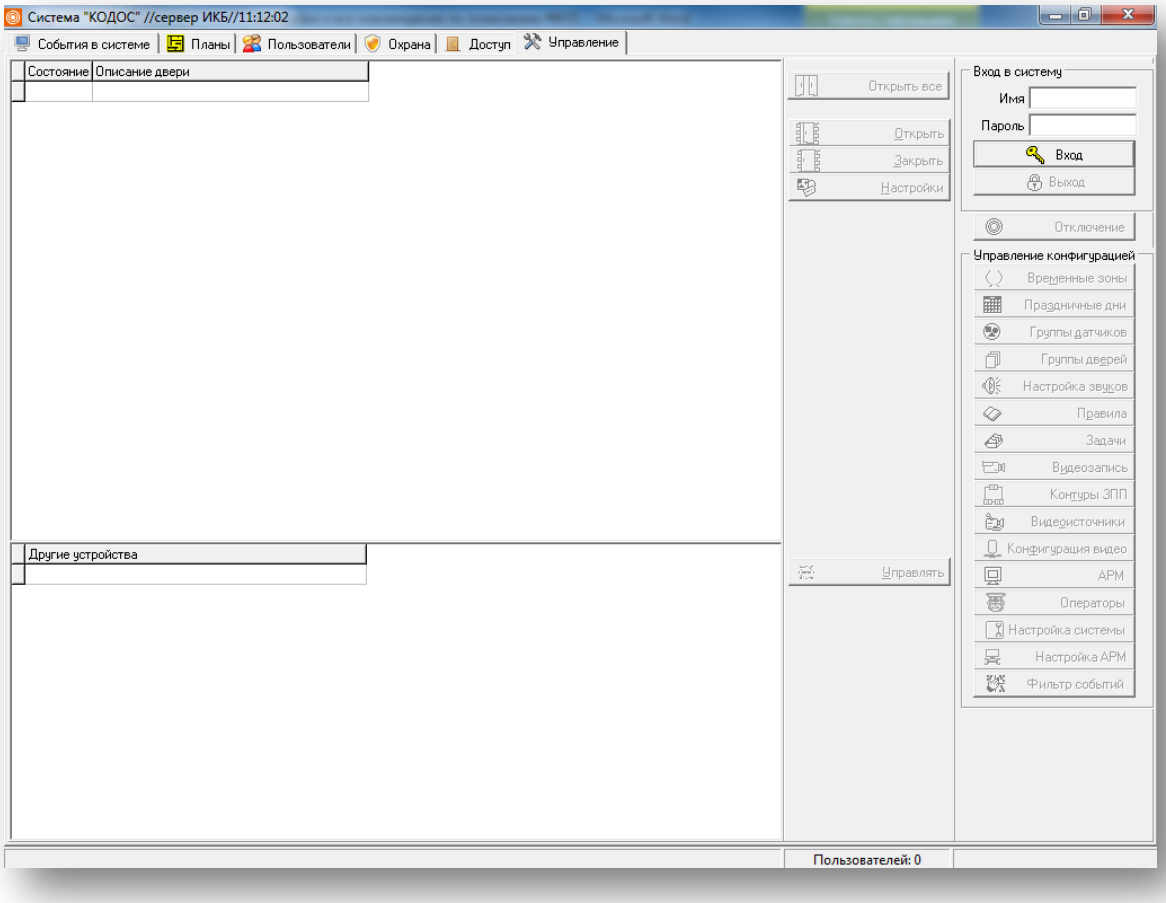
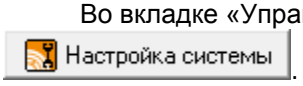


Рисунок 3.1

- В разделе «Вход в систему» введите имя и пароль администратора. По умолчанию установлены: имя — admin, пароль — power.

3.2 Настройка системы

Во вкладке «Управление» в разделе «Управление конфигурацией» нажмите кнопку 

.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.2.1 Вкладка «Основные параметры»

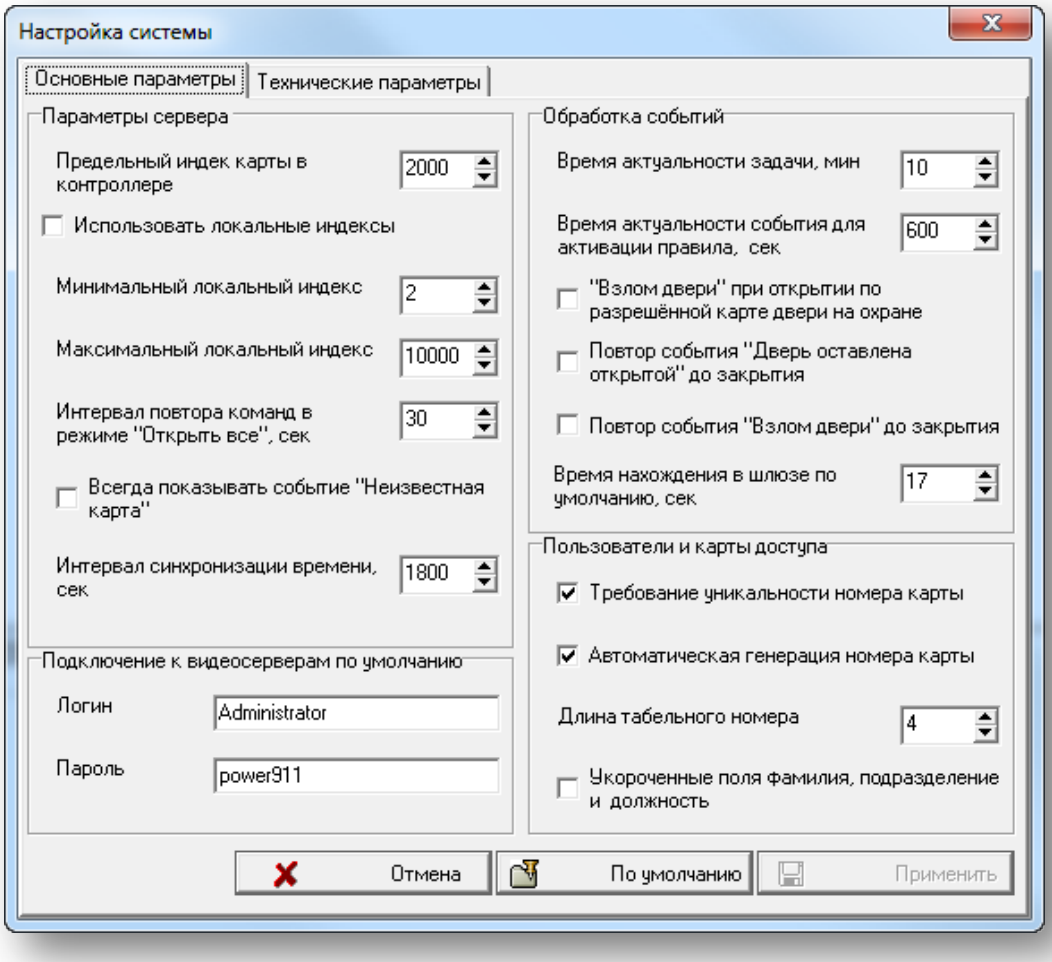


Рисунок 3.2

Раздел «Параметры сервера»

- «Предельный индекс карты в контроллере» — параметр определяет количество карт, которые могут быть записаны в память контроллера. Значение этого параметра должно совпадать с распределением памяти в контроллере.
- «Использовать локальные индексы» — функцию рекомендуется использовать, если количество карт пользователей, хранящихся в базе данных, больше, чем позволяет записать память контроллера.
- «Минимальный локальный индекс» — определяет количество карт доступа, заблокированных от удаления.
- «Максимальный локальный индекс» — значение, обозначающее верхний предел массива данных в контроллере.
- «Интервал повтора команд в режиме „Открыть всё“, сек» — интервал для широковещательной команды «Открыть всё».
- «Всегда показывать событие „Неизвестная карта“» — параметр, указывающий, всегда ли система должна показывать событие «Считана неизвестная карта», или только при отсутствии её кода в базе данных.

  Если карта прописана в базе данных, но эти сведения не были внесены в контроллер — при установленном флаге ИКБ будет выдавать событие «Неизвестная карта». Если флаг не установлен, придет событие «Запрещенная карта».

- Интервал синхронизации времени, сек» — каждый раз в указанный период во все контроллеры прописывается текущее системное время.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Раздел «Подключение к видеосерверам по умолчанию»

Раздел предназначен для подключения интегрированного видео. Поля «Логин» и «Пароль» хранятся в базе данных системы и по умолчанию установлены:

- «Логин» — Administrator.
- «Пароль» — power911.

Значения полей «Логин» и «Пароль» можно задать и в программе «Конфигуратор» при редактировании свойств компьютера, однако, если в «Конфигураторе» не заданы иные значения, используются параметры, установленные по умолчанию.

Подробнее о настройке системы см. «Руководство оператора программы „Конфигуратор“.

Раздел «Обработка событий»

- «Время актуальности задачи, мин» — если при проверке списка задач на протяжении установленного периода есть те, которые в этот интервал не выполнялись, ИКБ начнет их выполнять.
- «Время актуальности события для активации правила, сек» — параметр, определяющий период времени, по истечении которого выполнение задачи нецелесообразно: например, если установлено правило срабатывания исполнительного устройства в ответ на какое-либо событие, но связи с контроллером нет продолжительное время, то после восстановления связи срабатывание исполнительного устройства уже не актуально.
- «„Взлом двери“ при открытии по разрешенной карте двери на охране» — параметр, определяющий появление события «Взлом двери» при открытии по разрешенной карте, если дверь на охране. Этот параметр не влияет на включение тревоги при открытии двери без карты.
- «Повтор события „Дверь оставлена открытой“ до закрытия» — при установленном флаге ИКБ будет генерировать это событие вплоть до закрытия двери.
- «Повтор события «„Взлом двери“ до закрытия» — при установленном флаге ИКБ будет генерировать событие «Взлом двери» пока дверь не снимут с охраны или не закроют.
- «Время нахождения в шлюзе по умолчанию, сек» — параметр, определяющий время нахождения пользователя в шлюзе в секундах. Если пользователь находится внутри шлюза больше установленного времени, то система не откроет вторую дверь. Она предоставит пользователю возможность выйти из шлюза только через ту дверь, через которую он вошел.

Раздел «Пользователи и карты доступа»

- «Требование уникальности номера карты» — установка флага определяет необходимость назначения каждому пользователю системы уникального табельного номера.
- «Автоматическая генерация номера карты» — установка флага означает автоматически назначаемый табельный номер при создании учетной записи пользователя.
- «Длина табельного номера» — параметр, определяющий количество символов в номере. Значение по умолчанию равно 4.
- «Укороченные поля фамилия, подразделение и должность» — ограничение количества вводимых символов в этих полях.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3.2.2 Вкладка «Технические параметры»

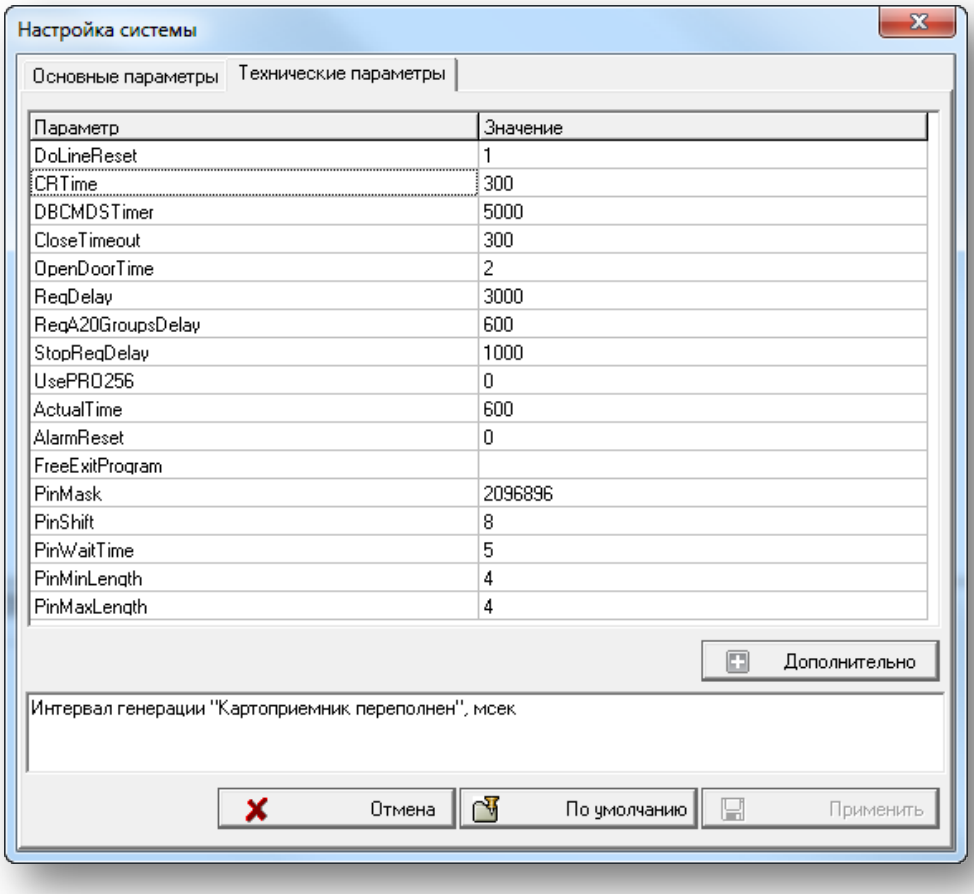


Рисунок 3.3

Имя	По умолчанию	Описание
DoLineReset	1	Значение этого параметра сообщает системе, делать или нет рестарт линии при потере связи с контроллерами (1 или 0 соответственно), по умолчанию значение параметра равно 1.
CRTime	300	Этот параметр нужен при работе с картоприёмником. Значение параметра — это количество мсек, в течение которых при считывании в картоприёмнике одинакового кода карты будет выдаваться событие «Картоприёмник переполнен».
DBCMDSTimer	5000	Параметр, определяющий интервал опроса команд в очереди DBCMDS, мсек. Частота опроса влияет на скорость, с которой изменения с клиентских приложений попадают на сервер и к устройствам. Значение параметра, установленное по умолчанию, менять не рекомендуется.
CloseTimeout	300	Параметр, определяющий интервал в секундах, в течение которого ожидается событие «Дверь открыта», прежде чем в системе появится сообщение о закрытии двери.
OpenDoorTime	2	Максимальный интервал для открытия двери по сливу событий с контроллера, мин
ReqDelay	3000	Время до начала инициализации контроллеров, мсек
ReqA20GroupsDelay	600	Параметр, определяющий время до начала опроса конфигурации Пульта A20, сек
StopReqDelay	1000	Параметр указывает время задержки между отправлениями команд выключения опроса сетевого контроллера, мсек
UsePRO256	0	Опция, позволяющая расширить настроенный диапазон уровней доступа и временных зон до 256. Для работы в этом режиме нужна

SEC.RU | Короткий путь к информации Скачано с sec.ru

		специальная прошивка для контроллера PRO.
ActualTime	600	Интервал проверки актуализации датчиков, сек
AlarmReset	0	В ИКБ после снятия тревоги с ППКОП А-20 постановка датчика на охрану зависит от значения, установленного для параметра AlarmReset: 0 — датчик ставится на охрану, если был в тревоге/ не было связи/ обрыв/ короткое замыкание; 1 — датчик ставится на охрану, если был в тревоге; 2 — датчик ставится на охрану, если не было связи/ обрыв/ короткое замыкание; 3 — ничего не делает.
FreeExitProgram	1	Закрытие программы без требования наличия данного права у оператора

Для более тонкой настройки системы нажмите кнопку 

. В открывшемся окне (Рисунок 3.4) введите нужный параметр. Для получения подробной консультации касательно дополнительных системных настроек обратитесь в отдел технической поддержки Компании.

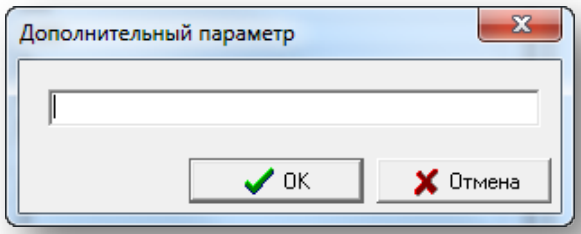
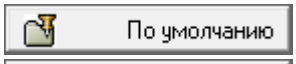
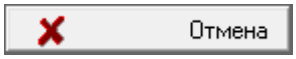
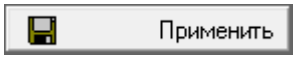


Рисунок 3.4

- Нажатие кнопки 

восстанавливает настройки, установленные по умолчанию.
- Нажатие кнопки 

отменяет внесенные в настройки изменения.
- Нажатие кнопки 

устанавливает введенные значения.

3.3 Создание списка операторов

В окне «Список операторов системы» (Рисунок 3.5):

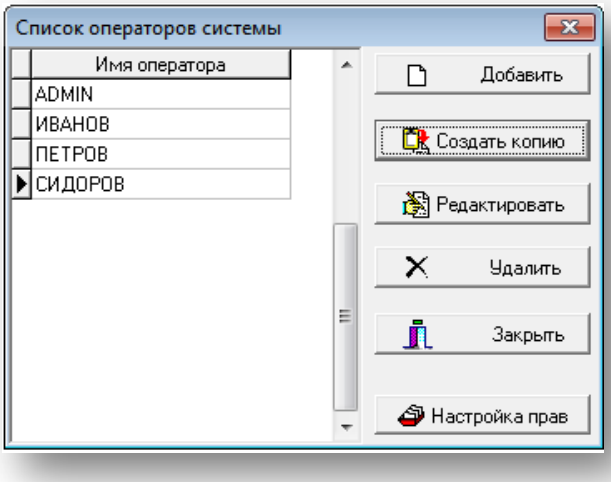
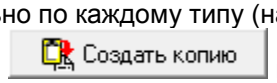


Рисунок 3.5

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- Кнопка 

позволяет добавить нового оператора (Рисунок 3.7). В открывшемся окне администратор задаёт новому оператору пароль, а также назначает права по управлению системой. Существует возможность выставлять их как группами, например «Права, связанные с видео», так и отдельно по каждому типу (например, «Просмотр видео по данным из архива»).
- Кнопка 

позволяет создать пользователя, имеющего такой же набор прав, что и выделенный оператор (Рисунок 3.6). Для этого одинарным щелчком левой кнопки мыши в окне «Список операторов системы» (Рисунок 3.5) следует выделить оператора, копию которого требуется создать. Затем нажать кнопку «Создать копию» и в открывшемся окне задать имя нового оператора.

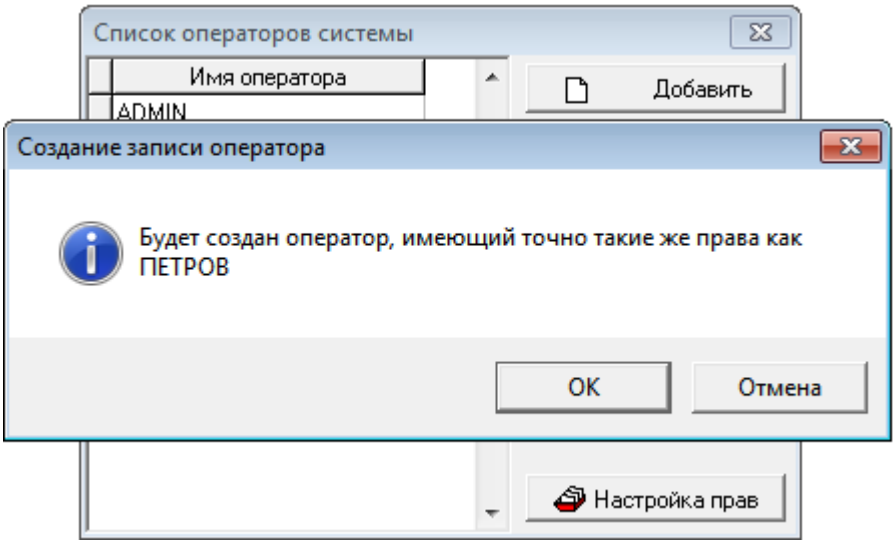
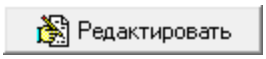
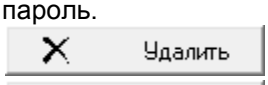
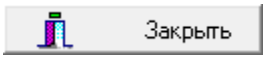
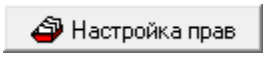


Рисунок 3.6

- Кнопка 

позволяет отредактировать права выбранного оператора и назначить ему другой пароль.
- Кнопка 

позволяет удалить выбранного оператора.
- Кнопка 

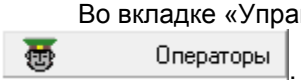
закрывает окно редактирования списка операторов системы.
- Кнопка 

даёт возможность назначать права операторам, учитывая привязку «оператор – организация».
-

ВНИМАНИЕ! Кнопка «Настройка прав» будет доступна только при наличии лицензии на модуль «Владельцы».

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.4 Назначение прав операторам

Во вкладке «Управление» в разделе «Управление конфигурацией» нажмите кнопку 

. В открывшемся окне «Изменить настройки оператора» администратор системы или оператор с правами администрирования может устанавливать и изменять права другим операторам.

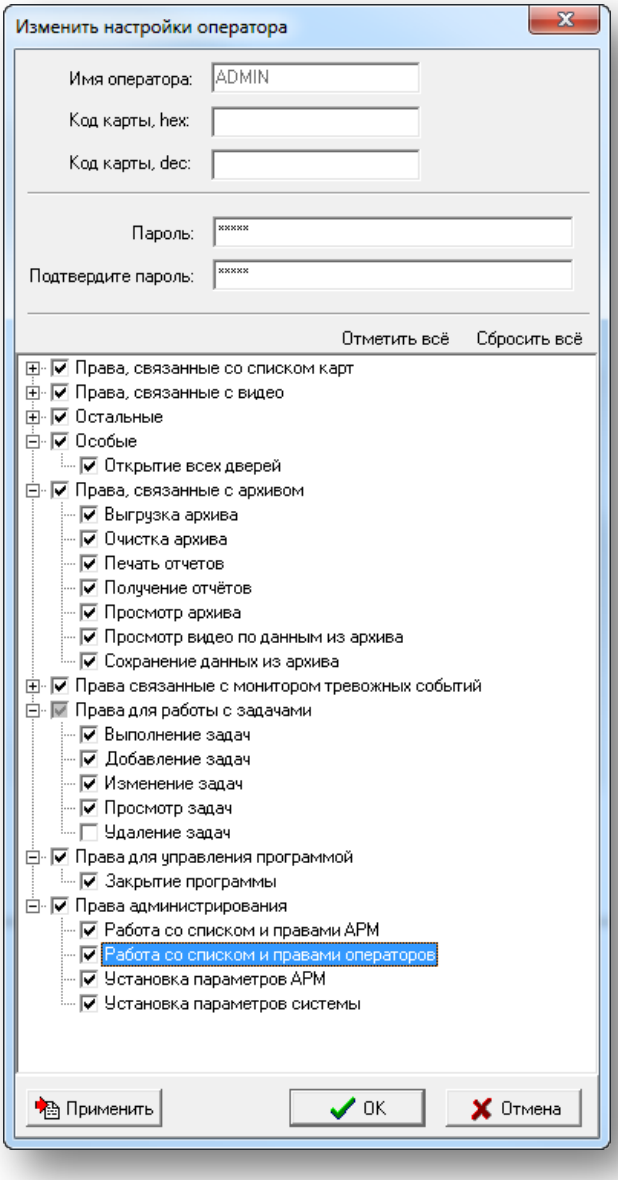


Рисунок 3.7

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Раздел «Права, связанные со списком карт»

- **«Добавление пользователей»** — оператору с установленным правом будет доступна кнопка «Добавить» во вкладке «Пользователи».
- **«Добавление пользователей (частичное)»** — оператор сможет создавать новые учетные записи пользователей, если номер карты был заблаговременно распознан (считан), а также добавлять к ним комментарии. Кнопка «Добавить» во вкладке «Пользователи» будет доступна только при условии, если в списке прав этому оператору назначили также или право «Просмотр пользователей», или «Просмотр посетителей», или «Работа со списком гостевых карт».
- **«Добавление посетителей»** — во вкладке «Пользователи» с помощью кнопок «Добавить», «Редактировать» оператор может добавить посетителя или гостя. Во вкладке «Пользователи» → «Посетители» можно увидеть добавленную учетную запись гостя. Право «Добавление посетителей» нельзя использовать без прав «Добавление пользователей», «Полное редактирование пользователей» или «Работа со списком гостевых карт».
- **«Освобождение карт»** — право позволяет оператору стирать информацию выбранной из списка карты и делать её пустой гостевой. Кнопка «Освободить» во вкладке «Пользователи» → «Посетители» будет доступна, если совместно с правом «Освобождение крат» в списке также отмечены или «Просмотр пользователей», или «Просмотр посетителей», или «Работа со списком гостевых карт».
- **«Полное редактирование пользователей»** — право позволяет оператору изменять информацию в учетной карте пользователя и редактировать группы пользователей (вкладка «Пользователи» → «Посетители» → кнопка «Группы»). Кнопка «Редактировать» во вкладке «Пользователи» → «Посетители» будет доступна при условии, если оператору также назначены права «Просмотр пользователей», «Просмотр посетителей» или «Работа со списком гостевых карт».
- **«Просмотр пользователей»** — во вкладке «Пользователи» → «Посетители» оператору будет доступен просмотр списка сотрудников.
- **«Просмотр посетителей»** — во вкладке «Пользователи» → «Посетители» оператору будет доступен просмотр списка гостей и посетителей.
- **«Работа со списком гостевых карт»** — во вкладке «Пользователи» → «Посетители» оператор сможет работать со списком гостевых (освобожденных) карт.
- **«Удаление карт»** — во вкладке «Пользователи» кнопка «Удалить» будет активна при условии, если оператору также назначены либо «Просмотр пользователей», либо «Просмотр посетителей», либо «Работа со списком гостевых карт».
- **«Управление группами пользователей»** — оператор, которому назначено это право, может управлять группами пользователей. Во вкладке «Пользователи» кнопка «Группы» будет активна лишь при условии, если оператору также назначено право «Полное редактирование пользователей».
- **«Частичное редактирование пользователей»** — кнопка «Редактировать» во вкладке «Пользователи» будет активна при условии, если оператору также назначено право «Просмотр пользователей», «Просмотр посетителей» или «Работа со списком гостевых карт**».**

Раздел «Права, связанные с видео»

- **«Запись видео»** — право даёт оператору возможность открывать видео, привязанное к датчику (вкладка «Планы»), а также включать и останавливать запись видео из контекстного меню датчика. Для полной реализации права «Запись видео» оператору также необходимо назначить права «Просмотр видео» и «Переключение планов».
- **«Изменение размеров видеоокон»** — в контекстном меню датчика с привязанной видеокамерой оператору будут доступны опции «Увеличить окно в 2 раза» и «Уменьшить окно в 2 раза». Для реализации возможности изменять размеры видеоокон необходимо назначить оператору также права «Просмотр видео» и «Переключение планов».
- **«Назначение видеокамер»** — оператору также необходимо назначить право на переключение планов — во вкладке «Управление» будет активна кнопка «Видеозапись», а также во вкладке «Планы» оператор сможет назначать камеры из контекстного меню точки доступа.
- **«Настройка детектора движения»** — право даёт оператору возможность устанавливать настройки детектора движения.
- **«Настройка параметров видеоканала»** — обязательно при проверке должно быть право «Переключение планов» в разделе прав «Остальные». Если нет права «Настройка параметров видеоканала», то при вызове контекстного меню правой кнопкой мыши, значки «Регулировка скорости/ качества» и «Настройка видеосигнала» будут скрыты. Также, право «Настройка параметров видеоканала» не может работать без права на просмотр видео.
- **«Просмотр видео»** — право даёт возможность во вкладке «Планы» открыть видеоокно камеры, а также в контекстном меню точки доступа будет доступен пункт «Видеообзор». Для полной реализации права на просмотр видео оператору также необходимо назначить право на переключение планов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **«Просмотр видеоархивов»** — при открытии окна видеокамеры с вкладки «Планы» оператору будет доступен значок «Показать архив». Для полной реализации права необходимо, чтобы оператору были также назначены права на переключение планов и просмотр видео.
- **«Просмотр списка видеосерверов»** — право даёт оператору просматривать список видеосерверов; во вкладке «Управление» кнопки «Видеоисточники» и «Конфигурация видео» будут активны. Кроме того, в контекстном меню точки доступа на вкладке «Планы» пункт «Выбор конфигурации видео» будет активным. Для полной реализации права необходимо оператору назначить также право на переключение планов.
- **«Редактирование списка видеосерверов»** — право даёт возможность оператору изменять состав списка видеосерверов. Для полной реализации права на редактирование необходимо также назначить оператору право на просмотр списка видеосерверов.
- **«Экспорт изображений»** — при вызове архива видеозаписи с вкладки «Планы» будут отображаться кнопки «Запись кадр в файл», «Распечатать кадр», «Запись фрагмента архива в AVI», «Просмотр видео», «Просмотр видеоархивов».

Раздел «Остальные»

- **«Блокирование дверей»** — право даёт оператору возможность заблокировать выбранные точки доступа; во вкладке «Доступ» будет активна кнопка «Блокировать».
- **«Блокирование управления дверьми»** — право даёт оператору возможность заблокировать управление выбранными точками доступа; во вкладке «Доступ» оператору будет доступна кнопка «Блокировать управление».
- **«Конфигурирование пультов»** — во вкладке «Управление» кнопка «Настройка пультов» активна, что даёт оператору возможность изменять настройки ППКОП А-20.
- **«Настройка звукового сопровождения»** — право даёт оператору возможность изменять настройки звукового сопровождения; во вкладке «Управление» кнопка «Настройка звуков» будет активна.
- **«Отмена свободного доступа»** — во вкладке «Доступ» будет активна кнопка «Закрыть свободный доступ», если до этого был включен свободный доступ.
- **«Переключение планов» —** право позволяет оператору переключать планы объекта.
- **«Постановка датчика на охрану» —** во вкладке «Доступ» в контекстном меню точки доступа пункт «Взять под охрану» будет активным.
- **«Постановка разделов» —** право даёт оператору возможность управлять постановкой и снятием разделов с охраны; во вкладке «Управление» кнопка «Постановка разделов» активна.
- **«Просмотр временных зон» —** право даёт оператору возможность просматривать временные зоны и праздничные дни; во вкладке «Управление» кнопки «Временные зоны» и «Праздничные дни» активны.
- **«Просмотр контуров ЗПП» —** право даёт оператору возможность просматривать контуры ЗПП; во вкладке «Управление» кнопка «Контуры ЗПП» активна.
- **«Просмотр монитора» —** право позволяет оператору просматривать текущие события в системе; во вкладке «Управление» кнопка «Фильтр событий» активна и позволяет настраивать параметры фильтра.
- **«Разблокирование дверей» —** право даёт оператору возможность снять блокировку с выбранных точек доступа; во вкладке «Доступ» кнопка «Разблокировать» будет активна.
- **«Разблокирование управления дверьми» —** право позволяет оператору снимать блокировку управления выбранными точками доступа; во вкладке «Доступ» кнопка «Разблокировать управление» активна.
- **«Разрешение свободного доступа»** — право позволяет оператору назначать свободный проход в выбранные точки доступа; во вкладке «Доступ» кнопка «Открыть свободный доступ» активна.
- **«Редактирование временных зон» —** право даёт оператору возможность просматривать и редактировать временные зоны и праздничные дни; во вкладке «Управление» кнопки «Временные зоны» и «Праздничные дни» активны.
- **«Редактирование групп датчиков» —** право позволяет оператору изменять состав списка групп датчиков, а также добавлять в группу новые датчики; во вкладке «Управление кнопка «Группы датчиков» будет активна.
- **«Редактирование групп дверей» —** право даёт оператору возможность изменять состав списка групп дверей, а также добавлять в группу новые точки доступа; во вкладке «Управление кнопка «Группы дверей» будет активна.
- **«Редактирование контуров ЗПП» —** право позволяет оператору устанавливать настройки контуров запрета повторного прохода, включать или исключать из них точки доступа; во вкладке «Управление» кнопка «Контуры ЗПП» будет активна.
- **«Свойства датчика»** — право позволяет оператору просматривать и изменять свойства датчика в его контекстном меню во вкладке «Планы». Для полной реализации права необходимо также назначить оператору разрешение на переключение планов.
- **«Свойства двери» —** право даёт оператору возможность изменять настройки выбранной точки доступа; во вкладке «Управление» кнопка «Настройка» активна.
- **«Снятие датчика с охраны» —** право позволяет оператору снимать выбранный датчик с охраны; во вкладке «Доступ» в контекстном меню датчика пункт «Снять с охраны» будет активным.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- **«Снятие тревоги» —** во вкладке «Доступ» в контекстном меню точки доступа в тревоге пункт «Снять тревогу» будет активным.
- **«Управление группами датчиков» —** право позволяет оператору просматривать, создавать, удалять группы и входящие в них датчики, кнопка «Индикация» в окне «Группы датчиков/ Зоны охраны» активна. Для полной реализации права на управление группами датчиков необходимо также назначить оператору разрешение на редактирование групп датчиков.
- **«Управление группами дверей»** — право даёт оператору возможность просматривать группы дверей и входящие в них точки доступа; во вкладке «Управление» кнопка «Группы дверей» активна.
- **«Управление дверью» —** право позволяет оператору открывать или закрывать выбранную во вкладке «Управление» дверь**;** кнопки «Открыть» и «Закрыть» активны.
- **«Управление исполнительными устройствами» —** право позволяет оператору управлять выбранным исполнительным устройством; во вкладке «Управление» кнопка «Управлять» активна. Если оператору также назначено право «Переключение планов», во вкладке «Планы» в контекстном меню точки доступа пункты «Настройка» и «Свойства» будут активны.
- **«Управление обходами охранника» —** право даёт оператору возможность устанавливать настройки обхода охранника; во вкладке «Управление» кнопка «Обход охранника» активна.
- **«Управление правилами» —** право позволяет оператору создавать и редактировать правила; во вкладке «Управление» кнопка «Правила» активна.
- **«Управление режимом работы двери (день/ ночь)»** — право даёт оператору возможность с помощью кнопок «Дневной режим» и «Ночной режим» во вкладке «Доступ» управлять выбранными точками доступа в дневном и ночном режимах.

Раздел «Особые»

- **«Открытие всех дверей»** — право позволяет оператору открывать все двери; во вкладке «Управление» кнопка «Открыть все» становится активной.

Раздел «Права, связанные с архивом»

- **«Выгрузка архива» —** право позволяет оператору выгружать в папку архив выбранных событий; кнопка «Выгрузка архива» в окне «Архив событий» будет активной. Для полной реализации права необходимо назначить оператору также право на просмотр архива.
- **«Очистка архива» —** право даёт оператору возможность удалять архив событий; кнопка «Удаление из архива» в окне «Архив событий» будет активна. Для полной реализации права необходимо назначить оператору также право на просмотр архива.
- **«Печать отчетов»** — право позволяет оператору распечатать выборку архивных событий; кнопка «Печать отчета» в окне «Архив событий» будет активна. Для полной реализации права необходимо назначить оператору также право на просмотр архива.
- **«Получение отчетов»** — право позволяет оператору проводить статистический анализ, устанавливать режимы «Учет присутствия сотрудников», «Учет рабочего времени» и «Первый вход — последний выход». Для полной реализации права необходимо назначить оператору также право на «Просмотр архива».
- **«Просмотр архива» —** назначение этого права необходимо для того, чтобы оператор мог работать с архивом событий.
- **«Просмотр видео по данным из архива» —** право позволяет оператору просматривать видео по данным из архива (окно «Архив событий»). Для полной реализации права необходимо назначить оператору также право на просмотр архива.
- **«Сохранение данных из архива»** — право даёт оператору возможность создавать отчёты в формате MS Word и MS Excel; соответствующие кнопки в окне «Архив событий» будут активны. Для полной реализации права необходимо назначить оператору также право на просмотр архива.

Раздел «Права, связанные с монитором тревожных событий»

- **«Обработка тревожных событий» —** право позволяет оператору обрабатывать тревожные события; кнопки «Обработать» и «Обработать всё» во вкладке «Тревожные события» будут активны. Для полной реализации права необходимо назначить оператору также право на просмотр тревожных событий.
- **«Просмотр обработанных тревожных событий» —** право позволяет оператору просматривать обработанные тревожные события в системе; вкладка «Обработанные события» будет присутствовать. Для полной реализации права необходимо назначить оператору также право на просмотр тревожных событий.
- **«Просмотр тревожных событий» —** право необходимо назначать операторам, которые будут работать с тревожными событиями в системе.
- **«Редактирование фильтра монитора тревожных событий» —** право позволяет оператору определять условия выборки тревожных событий из списка; кнопка «Фильтр» во вкладке «Тревожные события»

SEC.RU | Короткий путь к информации Скачано с sec.ru

будет активна. Для полной реализации права необходимо назначить оператору также право на просмотр тревожных событий.

- **«Экспорт обработанных событий в MS Excel»** — право позволяет оператору выгружать обработанные события в формате MS Excel; кнопка «Экспорт в Excel» во вкладке «Обработанные» будет присутствовать. Для полной реализации права необходимо назначить оператору также право на просмотр тревожных событий.

Раздел «Права для работы с задачами»

- **«Выполнение задач» —** право позволяет оператору выполнять задачи из списка в окне «Планировщик задач»; кнопка «Задачи» во вкладке «Управление» будет активна. Для полной реализации права необходимо назначить оператору также разрешение на просмотр задач.
- **«Добавление задач» —** право даёт оператору возможность добавлять новые задачи; кнопка «Добавить» в окне «Планировщик задач» будет активна. Для полной реализации права необходимо назначить оператору также разрешение на просмотр задач.
- **«Изменение задач» —** право позволяет оператору изменять задачи из списка в планировщике задач. Для полной реализации права необходимо назначить оператору также разрешение на просмотр задач.
- **«Просмотр задач» —** право позволяет оператору просматривать список задач (кнопка «Задачи во вкладке Управление» → окно «Планировщик задач»).
- **«Удаление задач»** — право позволяет оператору удалять выбранные задачи; кнопка «Удалить» в окне «Планировщик задач» будет активна. Для полной реализации права необходимо назначить оператору также разрешение на просмотр задач.

Раздел «Права для управления программой»

- **«Закрытие программы»** — право даёт возможность оператору закрыть программу.

Раздел «Права администрирования»

- **«Работа со списком и правами АРМ»** — право даёт оператору возможность добавлять, изменять и удалять автоматизированные рабочие места, а также определять их настройки; во вкладке «Управление» кнопки «АРМ» и «Настройка АРМ» будут активны.
- **«Работа со списком и правами операторов» —** право позволяет добавлять новых операторов, назначать и изменять их права для работы с системой, определять их права для работы с организациями, а также задавать настройки автоматизированных рабочих мест. Во вкладке «Управление» кнопки «Операторы» и «Настройка АРМ» активны.
- **«Установка параметров АРМ» —** право позволяет оператору настраивать параметры автоматизированных рабочих мест. Во вкладке «Управление» кнопки «АРМ» и «Настройка АРМ» активны.
- **«Установка параметров системы»** — право позволяет оператору определять параметры системы и задавать настройки автоматизированных рабочих мест. Во вкладке «Управление» кнопки «Настройка системы» и «Настройка АРМ» активны.

3.5 Настройка модуля «Владельцы»

ВНИМАНИЕ! Работа с модулем «Владельцы» возможна только при наличии лицензии на него.

Модуль «Владельцы» предназначен для разграничения прав доступа операторов к различным объектам в ИКБ «КОДОС» Например, при использовании несколькими организациями или разными подразделениями одной организации единого сервера.

Для работы с модулем «Владельцы» необходимо предварительно настроить список организаций в программе «Конфигуратор» (подробнее см. «Руководство оператора программы „Конфигуратор“».).

Администратор системы (пользователь «admin») по умолчанию имеет права доступа на все элементы системы (двери, датчики, устройства, пользователей), независимо от их принадлежности к той или иной организации.

SEC.RU | Короткий путь к информации Скачано с sec.ru

ВНИМАНИЕ! Перед тем как назначать права операторам на управление системой безопасности определенной организации, необходимо в программе «Конфигуратор» создать список организаций, а затем в программе «Сервер ИКБ» создать список операторов (см. п. Создание списка операторов) и назначить им права.

- Для настройки прав операторов по отношению к организациям нажмите кнопку «Настройка прав» в окне «Список операторов системы» (Рисунок 3.5).

ПРИМЕЧАНИЕ – Поскольку оператор может контролировать безопасность нескольких организаций, то в рамках одного объекта охраны для каждой организации оператору будут назначены индивидуальные права.

Окно определения прав доступа в модуле «Владельцы» состоит из двух основных областей: области списка организаций (**1**) и области списка операторов (**2**) (Рисунок 3.8).

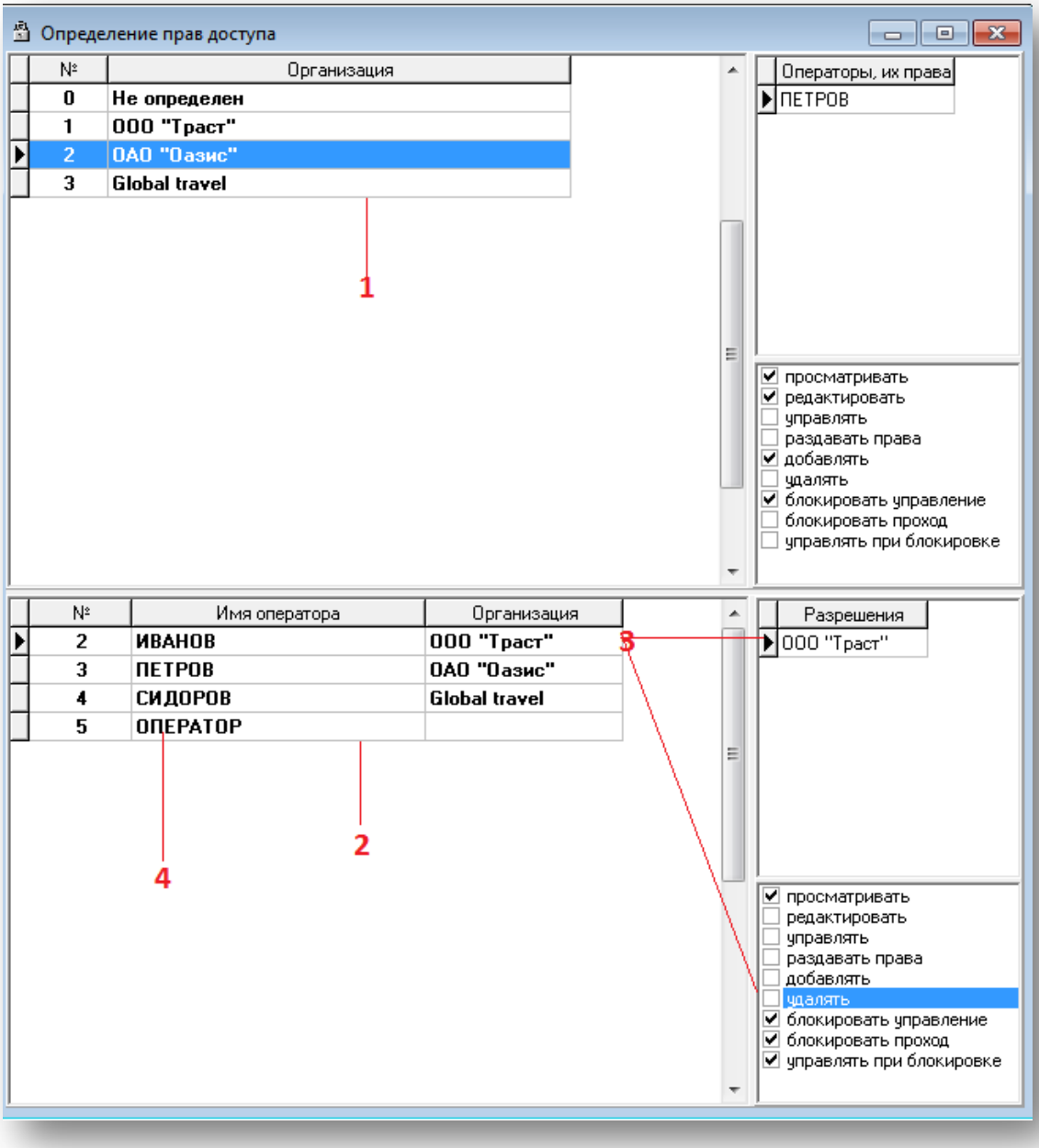


Рисунок 3.8

В области списка операторов отображаются права операторов для работы с определенной организацией (см. рисунок выше (**3**)).

- Новый оператор добавляется с характеристикой организации по умолчанию «Не определен» (Рисунок 3.9).
- Одинарным щелчком левой кнопки мыши по имени оператора — в разделе «Разрешения» отобразятся разрешенные действия выбранного оператора в организации.
- Оператору можно назначать права для работы с несколькими организациями. Список всех разрешенных организаций для текущего оператора показывается в графе «Разрешения» правой части области списка операторов

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Для изменения привязки оператора к организации необходимо двойным щелчком левой кнопки мыши по имени оператора в списке окна «Определение прав доступа» (Рисунок 3.8 (4)) вызвать окно «Изменение организации» (см. рисунок ниже). В выпадающем списке выбрать организацию.

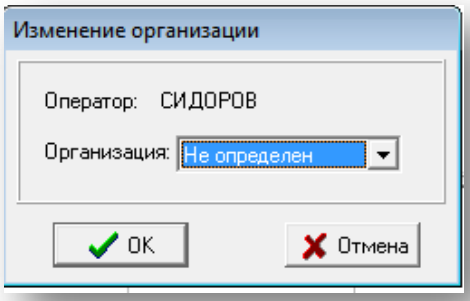


Рисунок 3.9

Список организаций (Рисунок 3.8 (1)) делится на две части: непосредственно список организаций (левая часть) и список операторов для выделенной организации (правая часть).

- Двойным щелчком левой кнопки мыши по строке с названием организации вызвать окно «Назначение прав для операторов в организации» (Рисунок 3.10).
- Для выбранной организации можно добавить любого оператора и установить ему индивидуальные права: нажмите кнопку «Добавить» → выберите в появившемся списке имя оператора → затем нажмите «ОК»).
- Кнопка Удалить удаляет выбранного оператора.

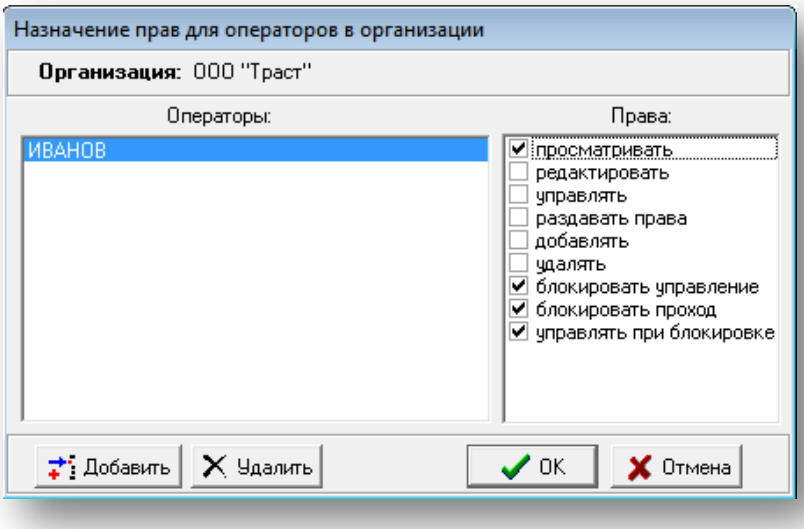


Рисунок 3.10

- Права просматривать, редактировать, добавлять, удалять распространяются на действия с картами пользователей.
- Право управлять разрешает проводить операции с оборудованием системы. Например, ставить и снимать датчики с охраны, открывать двери и т. д.

Оператор ИКБ может действовать в рамках прав, заданных при создании его учетной записи (Рисунок 3.7) и при определении его прав на работу с какой-либо организацией (Рисунок 3.10).

Оператор не сможет выполнять действие, запрещенное либо в его учетной записи, либо в модуле «Владельцы», даже если выполнение этого действия разрешено либо в учетной записи, либо в модуле «Владельцы».

Так, если в рамках учетной записи оператору определены только права, связанные с видео, а в модуле «Владельцы» допускается удаление и добавление карт, то оператор сможет действовать только в рамках прав, связанных с видео.

И наоборот:

SEC.RU | Короткий путь к информации Скачано с sec.ru

Если в модуле «Владельцы» у текущего оператора нет права на редактирование карты в рамках работы с определенной организацией, он не сможет редактировать карты, даже если такая возможность определена ему правами операторской учётной записи.

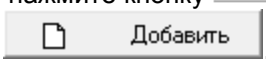
- При входе в программу оператору доступна только информация, на которую у него есть права (в свойствах оборудования или пользователя установлен та же организация).
- Группа дверей или группа датчиков создаются с признаком той же организации, что и текущий оператор. Это поле может редактировать только администратор системы (admin) и оператор с правами этой организации.
- При добавлении в группу дверей (датчиков) оператору доступен только список тех дверей (датчиков), на которые у него есть разрешения. Если датчик уже включен в группу, то при добавлении датчиков в группу, в списке выбора он не отображается.

3.6 Добавление АРМ

Клиентские приложения (например, программа «Администратор ИКБ»), подключенные к серверу, автоматически добавляют себя в список автоматизированных рабочих мест (АРМ) и используют настройки, установленные по умолчанию. Впоследствии этим АРМам можно задать индивидуальные настройки (см. п. 3.7).

Кроме того, АРМы можно добавлять из программы. Это может быть полезным на этапе проектирования, если сетевое подключение между сервером и клиентом еще не установлено. В этом случае для добавления каждого рабочего места необходим свой USB-ключ защиты.

- Вставьте USB-ключ защиты.
- Во вкладке «Управление» в разделе «Управление конфигурацией» нажмите кнопку 

.
- В открывшемся окне «Список АРМ» (Рисунок 3.11) нажмите кнопку 

.

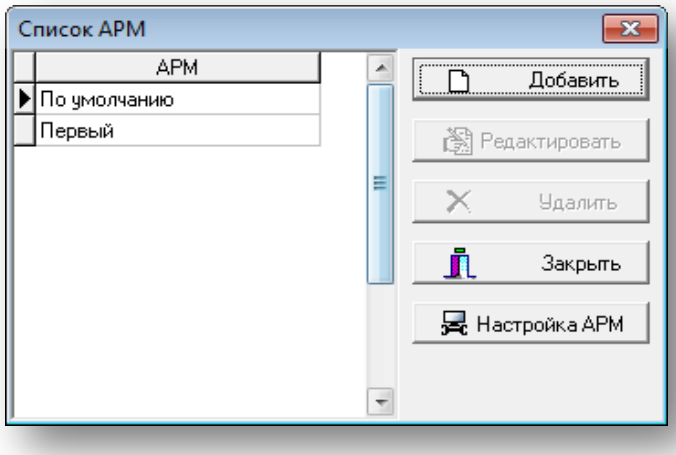


Рисунок 3.11

- В окне «Добавить/ Изменить АРМ» (Рисунок 3.12) введите название рабочего места, затем нажмите кнопку  «Выбрать номер ключа из подключенных».

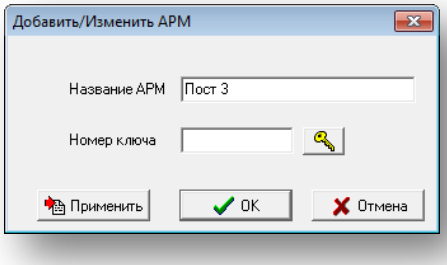


Рисунок 3.12

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- В окне «Ключи» (Рисунок 3.13) выделите нужный код ключа и нажмите кнопку «Выбрать».

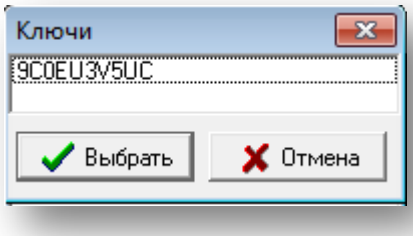
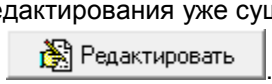


Рисунок 3.13

- Выбранный код появится в поле «Номер ключа» в окне «Добавить/ Изменить АРМ» (Рисунок 3.12). Затем нажмите «ОК».

Если Вы ошиблись при вводе или забыли внести номер ключа, появится окно-предупреждение:

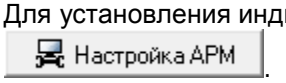
При введении номера уже существующего ключа программа также выдаст предупреждение.

- Нажмите «ОК» и повторите ввод номера ключа.
- Для редактирования уже существующего АРМ выделите его название в окне «Список АРМ» и нажмите кнопку 

. В открывшемся окне «Добавить/ Изменить АРМ» внесите нужные коррективы.
- Для удаления выделите название АРМ в списке и нажмите кнопку 

. В открывшемся окне нажмите «Да».
- Для закрытия окна «Список АРМ» нажмите кнопку 

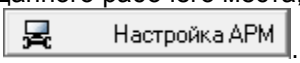
.

- Для установления индивидуальных параметров работы выбранного рабочего места нажмите кнопку 

.
- Окно «Настройка АРМ #имя выбранного в списке рабочего места» (Рисунок 3.14) предназначено для настройки параметров АРМ администратором или оператором, имеющим право на «Установку параметров АРМ» (подробнее о назначении прав операторам см. п. Назначение прав операторам).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.7 Настройка АРМ

Для того чтобы сконфигурировать систему определенным образом для заданного рабочего места, во вкладке «Управление» в разделе «Управление конфигурацией» нажмите кнопку 

.

3.7.1 Вкладка «Локальные параметры»

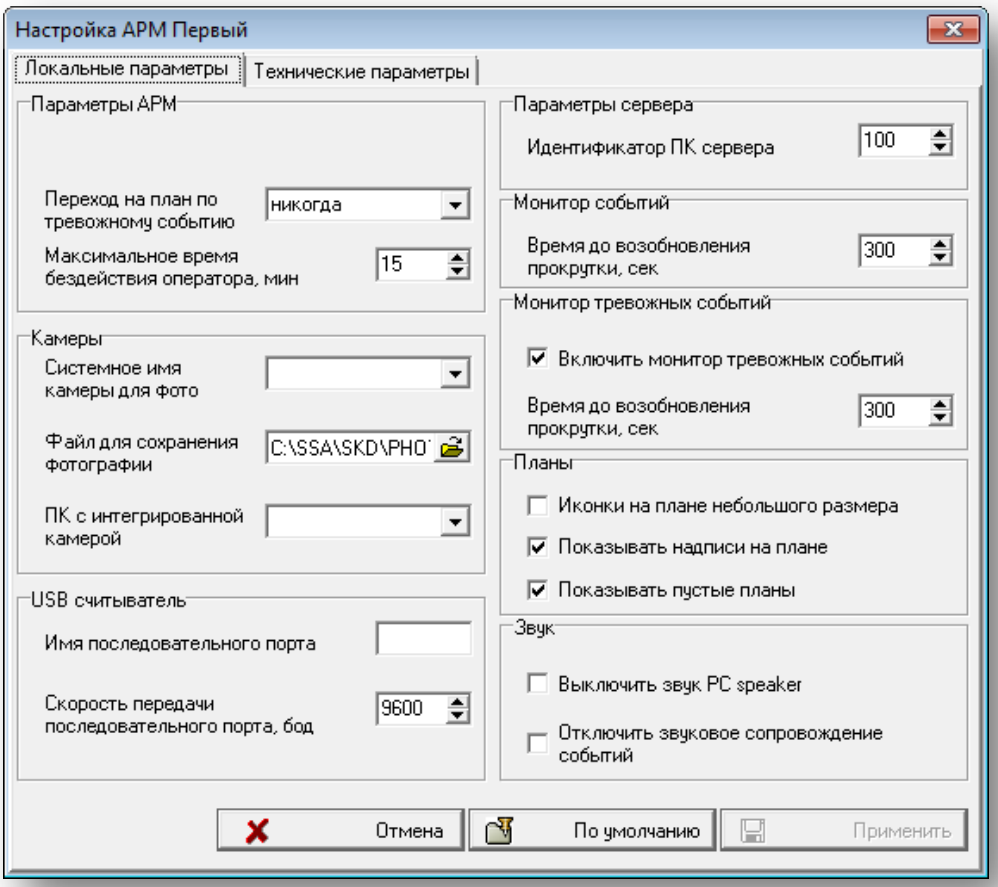


Рисунок 3.14

Раздел «Параметры АРМ»

- «При потере связи с БД» — из выпадающего списка выберите предложенное действие (уведомление, закрытие или перезагрузка), которое будет выполнять система при потере связи с базой данных.
- «Переход на план по тревожному событию» — из выпадающего списка выберите предложенное условие (всегда, никогда, если активна вкладка), при котором ИКБ покажет соответствующий план в ответ на тревожное событие (срабатывание датчика/ взлом двери/ событие «Дверь оставлена открытой»).
- «Максимальное время бездействия оператора» — время до выхода в безоператорный режим.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Раздел «Камеры»

- «Системное имя камеры для фото» — имя источника видеоизображения. Параметр требуется для «Модуля персонализации карт» при добавлении фотографии пользователю.
- «Файл для сохранения фотографии» — в поле укажите путь для сохранения фотографии.
- «ПК с интегрированной камерой» — из выпадающего списка следует выбрать IP-адрес ПК с интегрированной камерой. Подробнее о добавлении видеоисточника к ПК см. «Руководство оператора программы „Конфигуратор“»

Раздел «USB-считыватель»

- «Имя последовательного порта» — укажите в поле номер COM-порта, к которому подключен USB-считыватель.
- «Скорость передачи последовательного порта, бод» — параметр определяющий скорость работы через COM-порт при подключенном USB-считывателе. Установленное по умолчанию значение менять не рекомендуется.

Раздел «Параметры сервера»

- «Идентификатор ПК сервера» — идентификатор ПК в программе «Конфигуратор», к которому привязано оборудование.

Раздел «Монитор событий»

- «Время до возобновления прокрутки, сек» — укажите время, по истечению которого новые события будут добавлены в список во вкладке «События в системе».

Раздел «Монитор тревожных событий»

- «Включить монитор тревожных событий» — если флаг не установлен, вкладка «Тревожные события» не будет отображена; тревожные события, накопившиеся в то время, пока был отключен «Тревожный монитор», не попадут в список «Необработанные события». Для того чтобы изменения вступили в силу, следует перезагрузить программу.
- «Время до возобновления прокрутки» — укажите время, по истечению которого новые события будут добавлены в список во вкладке «Тревожные события».

Раздел «Планы»

- «Иконки на плане небольшого размера» — параметр, позволяющий уменьшить размер ярлыков датчиков на плане. Для того чтобы изменения вступили в силу, следует перезагрузить программу.

- «Показывать надписи на плане» — при установленном флаге номера датчиков на плане будут отображены.
- «Показывать пустые планы» — если на плане нет объектов, видимых данному оператору, планы не будут видны при установленном флаге.

Раздел «Звук»

- «Выключить звук PC speaker» — установите флаг для включения оповещений.
- «Отключить звуковое сопровождение событий» — для отключения установите флаг.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3.7.2 Вкладка «Технические параметры»

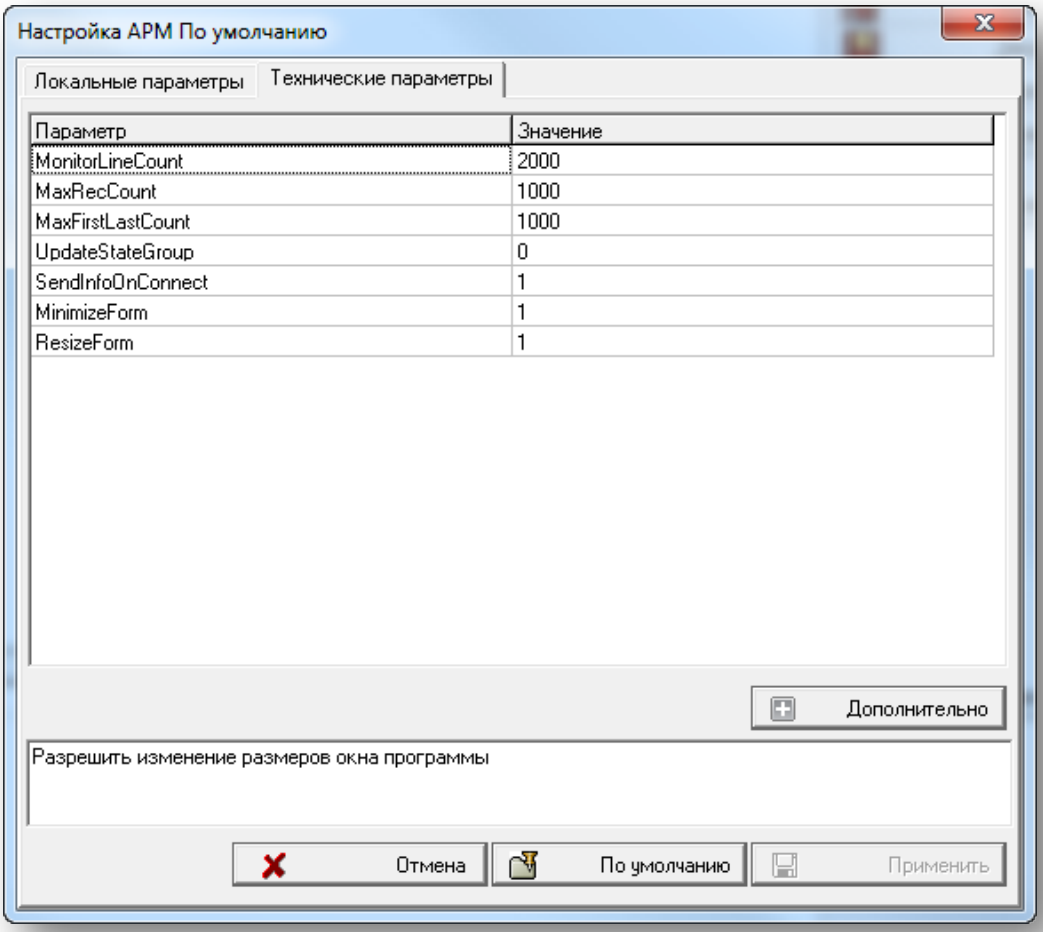
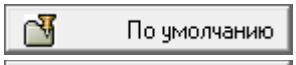


Рисунок 3.15

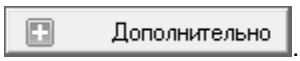
Имя	По умолчанию	Описание
MonitorLineCount	2000	Параметр, определяющий количество строк в списке «События в системе»
MaxRecCount	1000	Максимальное число строк при просмотре
MaxFirstLastCount	1000	Параметр, определяющий количество пользователей, для которых формируется отчет «Первый вход - последний выход».
UpdateStateGroup	0	Параметр, определяющий наличие/ отсутствие кнопки «Обновить» во вкладке «Охрана». Если этому параметру установить значение «1», на клиенте во вкладке «Охрана» кнопка «Обновить» будет отображена. На сервере этой кнопки не будет.
SendInfoOnConnect	1	Отправлять уведомление о входе оператора
MinimizeForm	1	Разрешить сворачивать окно программы
ResizeForm	1	Разрешить изменение размеров окна программы

- Нажатие кнопки 

восстанавливает настройки, установленные по умолчанию.
- Нажатие кнопки 

отменяет внесенные в настройки изменения.
- Нажатие кнопки 

устанавливает введенные значения.

Для более тонкой настройки системы нажмите кнопку 

. В открывшемся окне

SEC.RU | Короткий путь к информации Скачано с sec.ru

(Рисунок 3.16) введите нужный параметр. Для получения подробной консультации касательно дополнительных системных настроек обратитесь в отдел технической поддержки Компании.

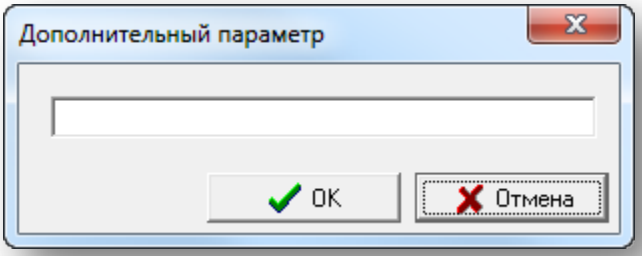


Рисунок 3.16

3.8 Настройка временных зон

Для настройки временных зон в разделе «Управление конфигурацией» нажмите кнопку 

.

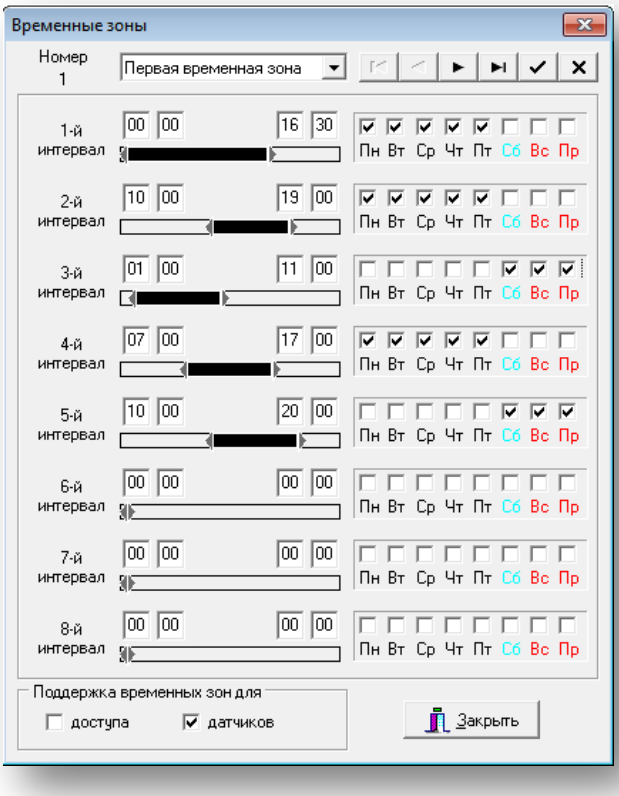


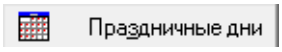
Рисунок 3.17

- В строке «Описание» (Рисунок 3.17) ввести название временной зоны либо оставить по умолчанию.
- Задать временные интервалы в строках «Начало» и «Окончание» (шаг — 10 минут).
- Установить дни действия временных интервалов флажками напротив дней недели и праздничных дней (Пр.), в которые действует данная временная зона.
- Установить флажок «Поддержка временных зон для доступа», если требуется включить поддержку временных зон для контроля доступа независимо от других установленных параметров, относящихся к временным зонам. В программе «Администратор ИКБ» данная функция доступна, если оператору задано соответствующее право.
- Установить флажок «Поддержка временных зон для датчиков», если требуется включить автоматическую постановку/ снятие датчиков по временным зонам независимо от других установленных параметров, относящихся к временным зонам. В программе «Администратор ИКБ» эта функция доступна, если у оператора есть соответствующее право.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Кнопка  сохраняет внесенные изменения.
- Кнопка  отменяет внесенные изменения.
- По завершении настроек нажать кнопку «Закрыть».

3.9 Настройка праздников

Для настройки работы системы безопасности по праздничным дням в разделе «Управление конфигурацией» нажмите кнопку 

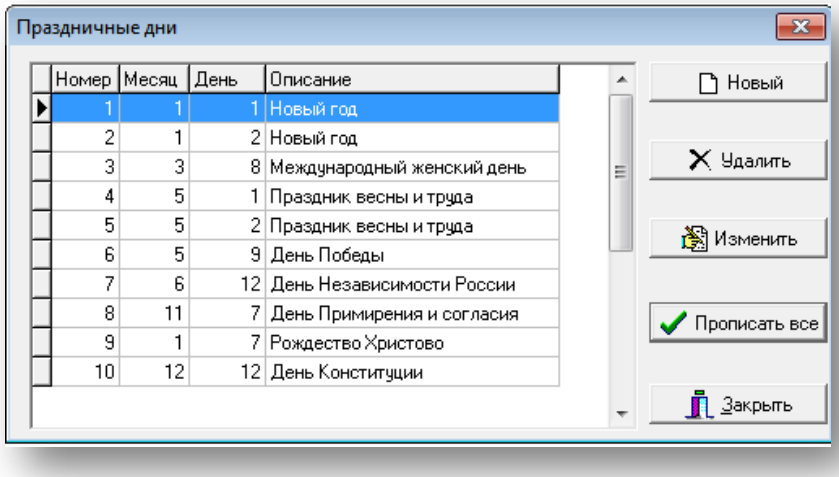


Рисунок 3.18

- Кнопка «Новый» предназначена для добавления нового праздника к уже заданным (Рисунок 3.19).

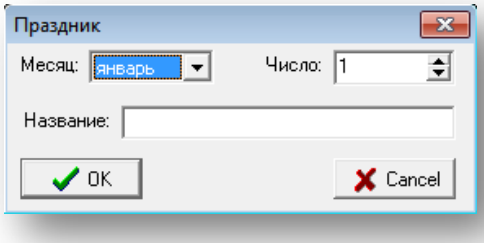


Рисунок 3.19

- Кнопка «Удалить» удаляет выделенный праздник из списка
- Кнопка «Изменить» позволяет редактировать имеющийся по умолчанию список государственных праздников.
- Кнопка «Прописать все» предназначена для ввода изменений в контроллеры, с которыми в настоящее время имеется связь.

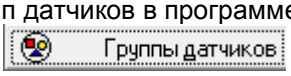
После внесения изменений нажать кнопку «Прописать все».

Будьте внимательны: если праздник выпадает на будний день или выходной, то разграничение доступа проводится в соответствии с настройками для праздничных дней.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3.10 Настройка групп датчиков

Для удобства управления, если в системе планируется установка большого количества датчиков (подключенные к адресным блокам А-06/2, А-06/8, А-07/4, А-07/8, А-09, датчики прохода и кнопки выхода контроллеров доступа), существует возможность объединять отдельные из них в группы.

Для создания групп датчиков в программе «Сервер ИКБ» во вкладке «Управление», в поле «Управление конфигурацией» нажать 

или кнопку «Настройка групп датчиков» в программе «Конфигуратор».

- В окне «Группы датчиков/ зоны охраны» (Рисунок 3.20) нажать кнопку  «Новая группа».

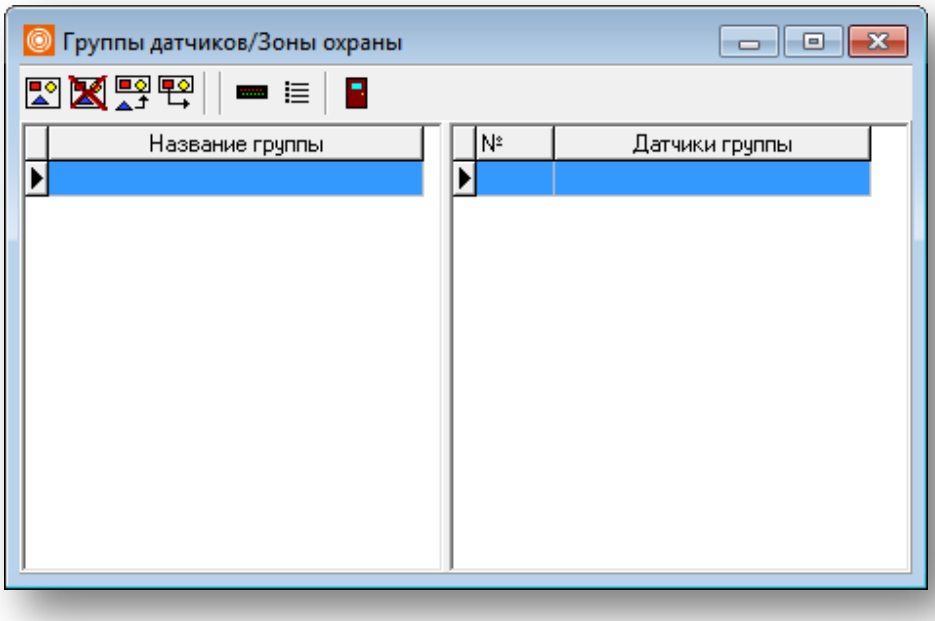


Рисунок 3.20

В окне «Добавление новой группы» (Рисунок 3.21) следует указать имя новой группы датчиков.

- В поле «Организация» выбрать из выпадающего списка организацию, имеющую право работать с объединенными в группу датчиками.

ПРИМЕЧАНИЕ – Если модуль «Владельцы» не установлен, то этот параметр носит информативный характер и не влияет на права доступа операторов.

- В поле «Объект» указать территориальное расположение датчиков.
- В поле «Зона охраны» можно новую группу датчиков привязать к одной из заранее созданных в «Конфигураторе» зон охраны — тогда на плане она будет отображаться графически. Причем важно учитывать, что одной группе датчиков можно назначить только одну зону охраны, и при создании другой группы датчиков в выпадающем списке «Зона охраны» назначенная предыдущей группе зона охраны отображаться уже не будет.

ПРИМЕЧАНИЕ – Группа датчиков может не иметь привязки к зонам охраны.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

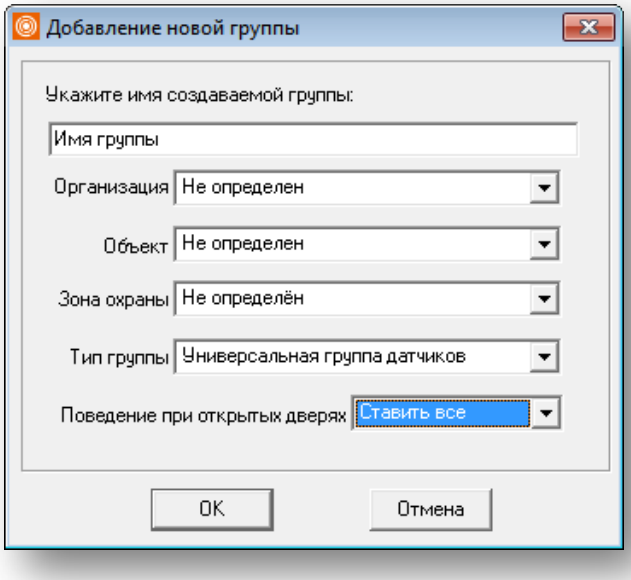


Рисунок 3.21

В выпадающем списке «Тип группы» следует выбрать позицию, которая определяется типом включенных в нее датчиков:

- «Зона охранной сигнализации» не может содержать пожарные датчики.
- «Зона тревожной сигнализации» не может содержать пожарные датчики.
- «Зона пожарной сигнализации» не может содержать иные датчики, кроме пожарных. Для данного типа группы невозможно выполнение команд «постановка на охрану» и «снятие с охраны».
- «Универсальная группа датчиков» не содержит ограничений по типам датчиков.
- «Технологическая группа датчиков» не содержит ограничений по типам датчиков. Данная группа не отображается в списке зон (групп) во вкладке «Охрана». Предназначена для создания групп датчиков, которые не используются для контроля состояния (норма-тревога-охрана) оператором, но при этом позволяют создавать правила.
- Для удаления группы датчиков/ Зоны охраны нажмите кнопку  «Удалить группу». В появившемся окне с предупреждением нажмите «Да».
- Для добавления в группу датчиков нажмите кнопку  «Добавить в группу» и выберите датчики для этой группы (Рисунок 3.22).

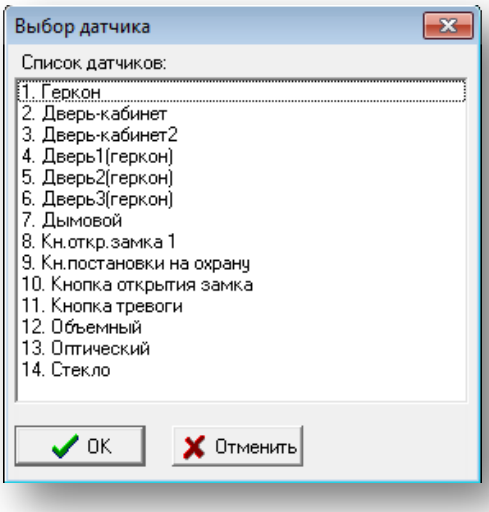


Рисунок 3.22

Затем — «ОК». Новая группа добавлена.

Для одновременного выбора нескольких датчиков используйте кнопки «Ctrl» или «Shift».

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Для удаления датчиков из группы нажмите кнопку «Удалить из группы». В появившемся окне с предупреждением нажмите «Да».
- Для настройки индикации выбрать группу и нажать «Индикация» в окне «Группы датчиков/ Зоны охраны» (Рисунок 3.20).

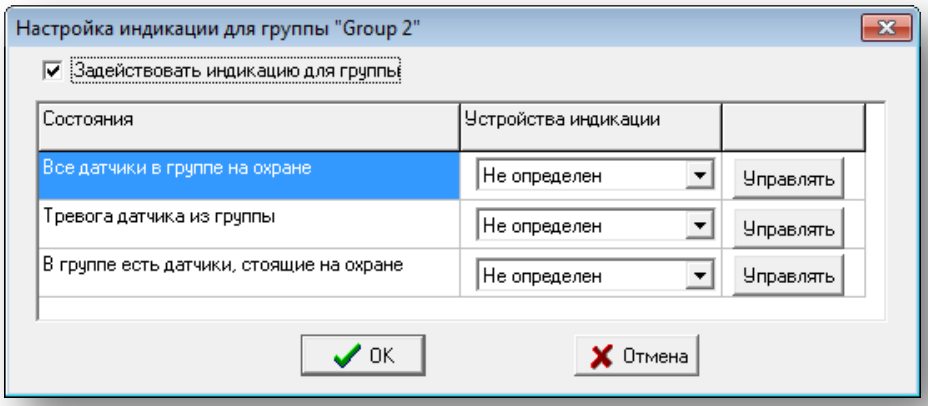


Рисунок 3.23

Для настройки индикации в окне (Рисунок 3.23) отметьте флагом «Задействовать индикацию для группы». Затем выберите состояния датчиков в группе и устройства индикации.

При нажатии кнопки «Управлять» появится окно (Рисунок 3.24) управления выбранным устройством индикации (кнопки «Включить» и «Выключить»). По завершении нажмите «Выход», затем «ОК».

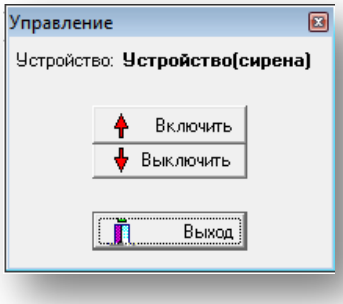


Рисунок 3.24

- Кнопка (Рисунок 3.20) открывает окно просмотра списка групп и типов датчиков в привязке к планам этажей.
- Кнопка «Выход» закрывает окно «Группы датчиков/ Зоны охраны».

3.11 Настройка групп дверей

При большом количестве дверей для удобства управления отдельные двери можно объединять в группы.

- Для создания групп дверей во вкладке «Управление», в поле «Управление конфигурацией» нажмите кнопку Группы дверей.

SEC.RU | Короткий путь к информации Скачано с sec.ru

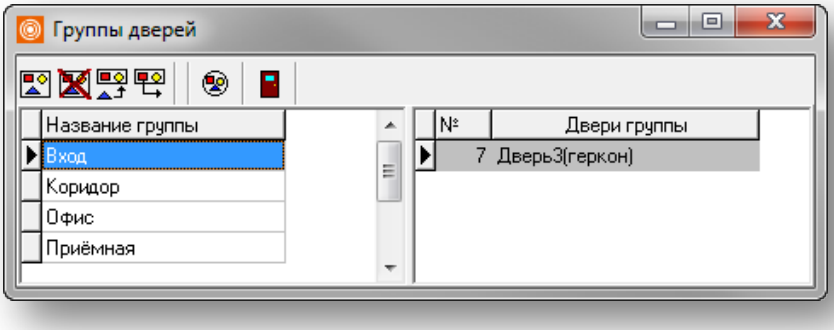


Рисунок 3.25

- Для добавления новой группы в окне «Группы дверей» (Рисунок 3.25) нажмите кнопку «Новая группа». В соответствующих полях (Рисунок 3.26) задайте имя создаваемой группы и организацию, которая имеет доступ к управлению этой группой дверей. Для операторов, не имеющих право работать с данной организацией, она в списке отображена не будет. Затем нажмите «ОК».

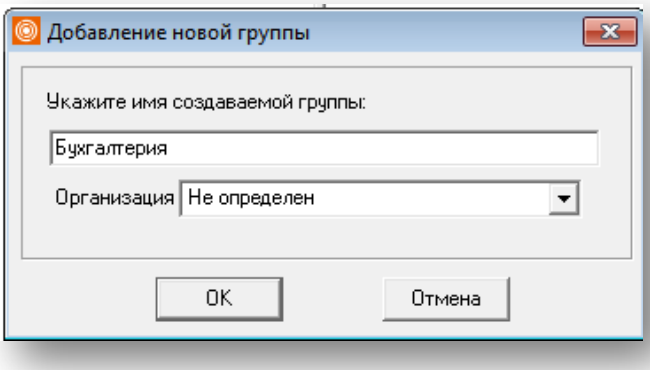


Рисунок 3.26

- Для удаления какой-либо группы следует выделить ее название в списке (Рисунок 3.25), а затем нажать кнопку «Удалить группу». В появившемся окне (Рисунок 3.27) нажмите «Да».

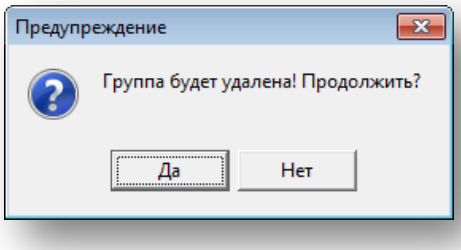


Рисунок 3.27

- Для добавления в группу новых дверей выберите название группы в списке и нажмите кнопку «Добавить в группу». В открывшемся окне «Выбор двери» (Рисунок 3.28) выберите одну или несколько (используя кнопки Ctrl или Shift) дверей, затем нажмите «ОК». Выбранные двери будут добавлены в группу.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

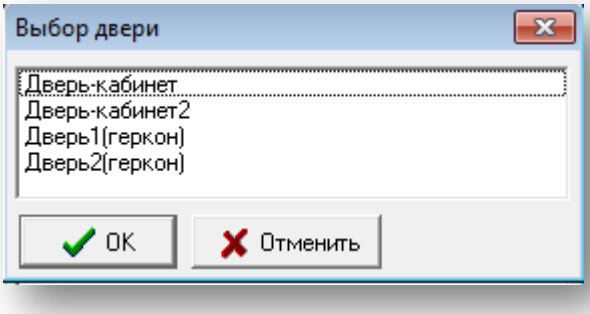


Рисунок 3.28

Если настройки двери отличаются от настроек группы, в которую планируется добавить эту дверь, то программа выдаст предупреждение (Рисунок 3.29).

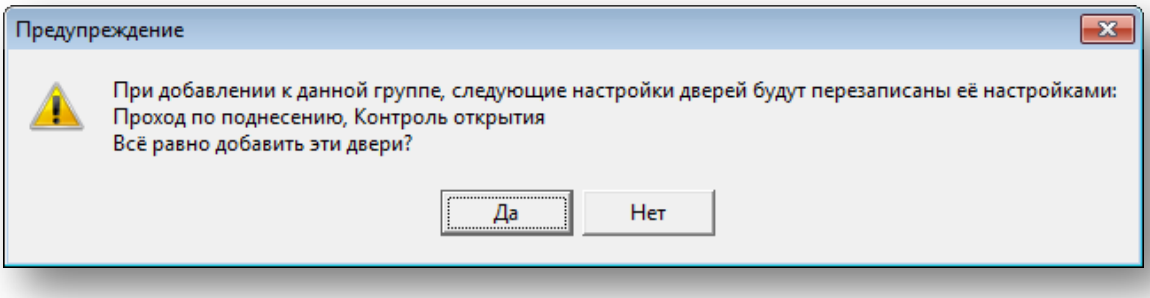


Рисунок 3.29

Если добавляемая дверь и группа принадлежат разным организациям, программа выдаст об этом предупреждение (Рисунок 3.30).

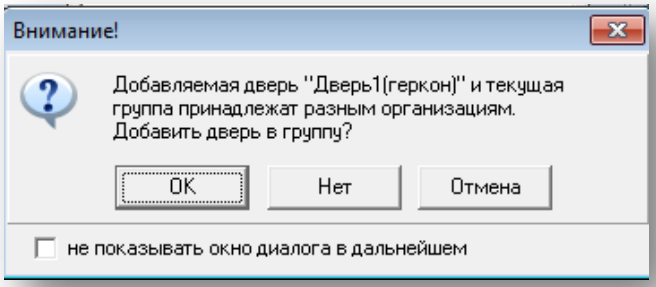


Рисунок 3.30

- Для удаления элементов из группы нажмите кнопку «Удалить из группы». В появившемся окне с предупреждением нажмите «Да».
- Двойным щелчком по названию группы в списке (Рисунок 3.25) или нажатием кнопки «Свойства группы» вызывается окно «Параметры групп дверей» (Рисунок 3.31), в котором можно отредактировать название группы, изменить привязку к организации и свойства группы. По завершении нажмите «ОК».

SEC.RU | Короткий путь к информации
Скачано с sec.ru

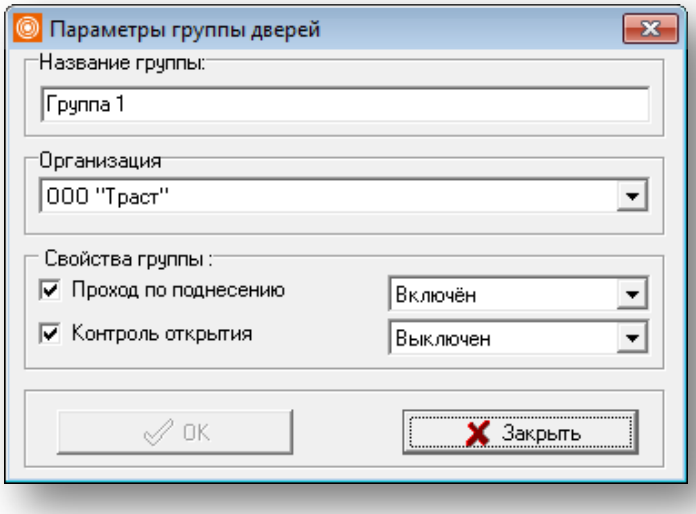


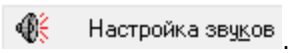
Рисунок 3.31

- Для выхода нажмите кнопку  «Выход».

3.12 Настройка звуков

В программе предусмотрена привязка звуковых файлов к системным событиям. Это необходимо для привлечения внимания оператора к работе системы.

Для настройки звукового сопровождения:

- Нажать во вкладке «Управление» в поле «Управление конфигурацией» .
- В окне «Звуковое сопровождение событий» (Рисунок 3.32) выбрать событие для редактирования.

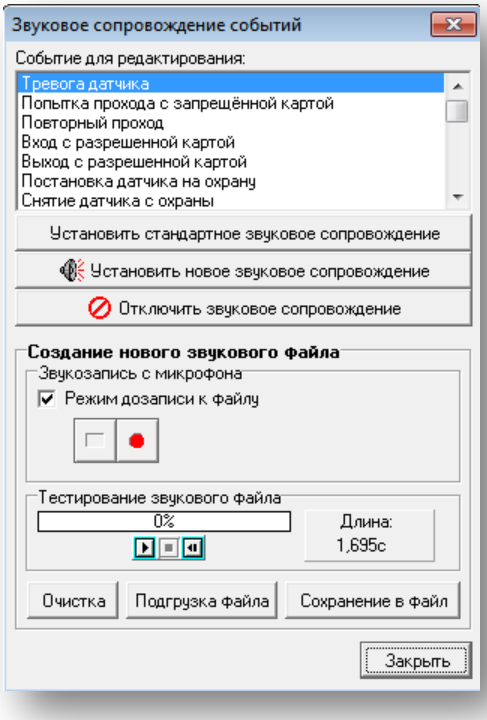


Рисунок 3.32

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- Прослушать звук с помощью кнопок в подразделе «Тестирование звукового файла».
- Назначить стандартный WAV-файл — «Установить стандартное звуковое сопровождение» или WAV-файл по выбору — «Установить новое звуковое сопровождение» и выбрать файл.
- В разделе «Создание нового звукового файла» можно записать новое звуковое сообщение
- В разделе «Звукозапись с микрофона» установите флажок «Режим дозаписи к файлу» и нажмите

  «Запись» .

- Продиктовав новое сообщение в микрофон, нажмите кнопку «Остановить запись» .
- Кнопка «Сохранение в файл» сохраняет запись в формате .WAV.
- Для отключения звукового сопровождения выбранного события нажмите

  Отключить звуковое сопровождение.
- Для замены старого звукового файла нажмите кнопку «Подгрузка файла» и в появившемся окне укажите папку, из которой следует выбрать новый WAV-файл.
- Кнопка «Очистка» удаляет временный звуковой файл.

3.13 Настройка правил

В ИКБ «КОДОС» существует возможность создавать правила, в соответствии с которыми система будет выполнять определенные действия в ответ на те или иные события.

Для настройки правил:

- Запустите «Сервер ИКБ», введите «Имя» и «Пароль». В группе «Управление конфигурацией» нажмите кнопку «Правила» — появится соответствующее окно (Рисунок 3.33).

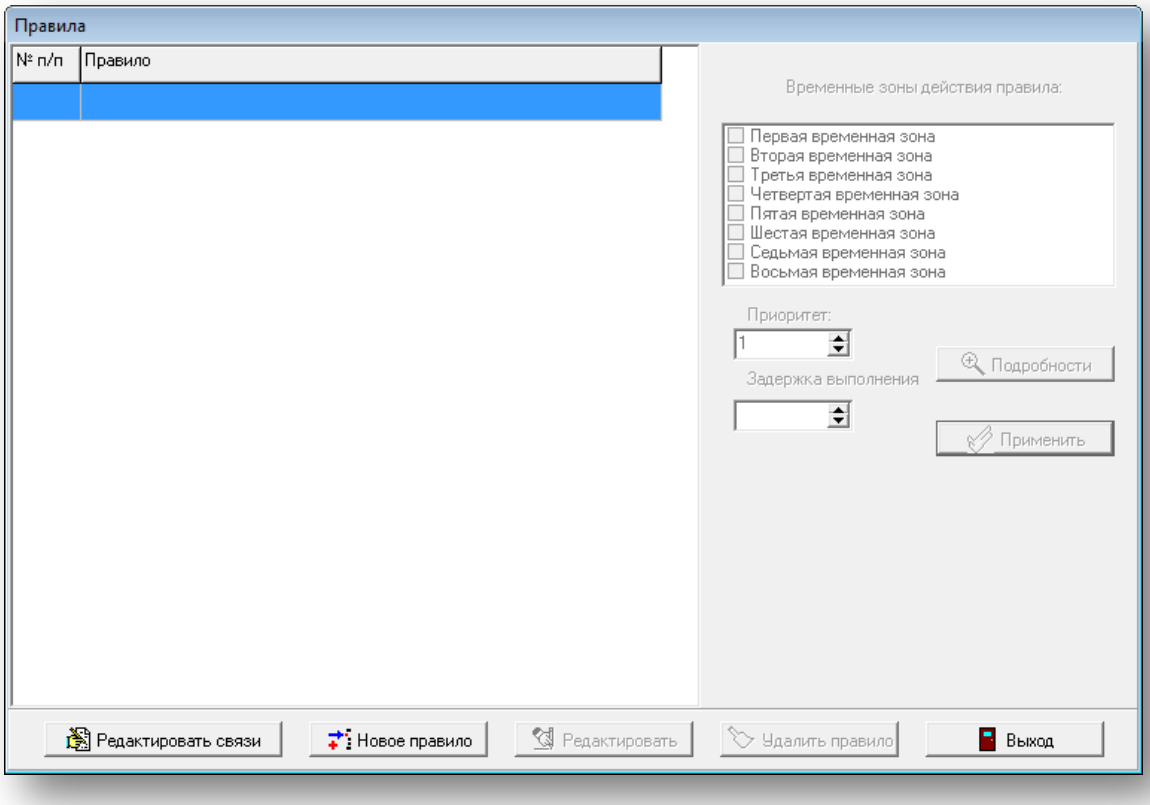


Рисунок 3.33

Для создания нового правила нажмите кнопку «Редактировать связи». Это позволит установить взаимосвязь между событием в ИКБ и вариантами возможных реакций (ответных действий) системы на них (Рисунок 3.34).

SEC.RU | Короткий путь к информации Скачано с sec.ru

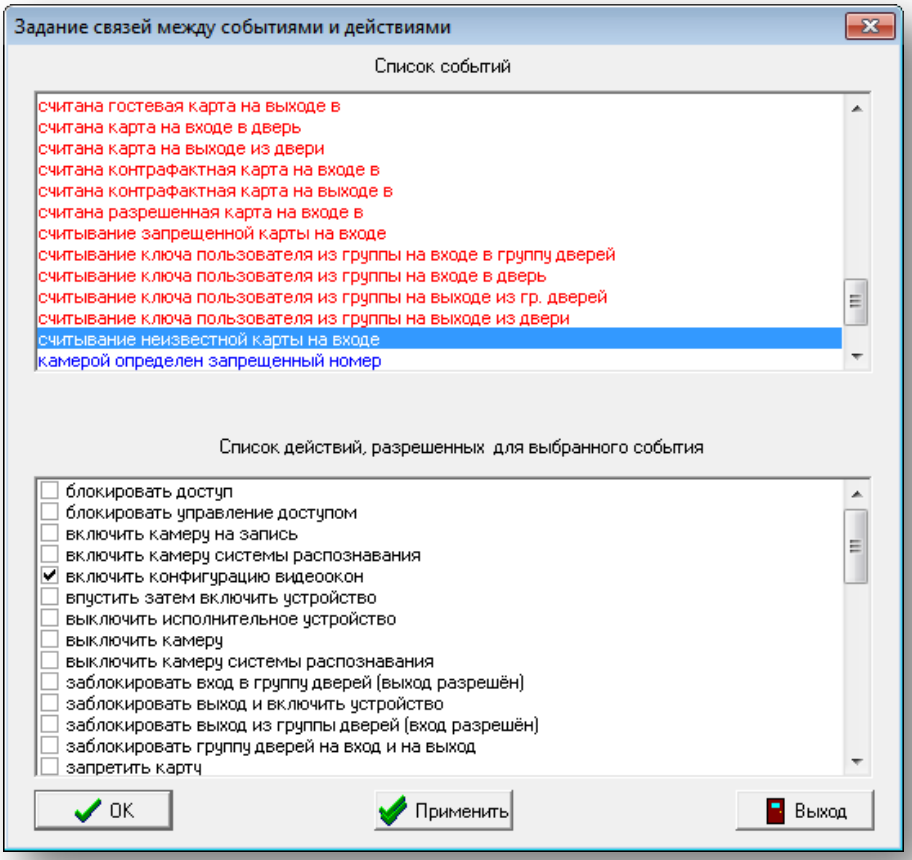


Рисунок 3.34

Одинарным щелчком левой кнопки мыши выберите из списка событий в верхней части окна требуемое и задайте ему из списка действий, разрешенных для выбранного события, соответствие. Для одного события можно назначить несколько разрешенных действий. Запоминание связей событий и действий осуществляется при нажатии кнопки «Применить».

Заданная таким образом связь между событием и действиями является «шаблоном» для правил, который в дальнейшем можно использовать несколько раз для различных объектов при создании правила.

ВНИМАНИЕ! При выборе соответствий между событиями или разрешенными действиями следует учитывать, способно ли устройство выполнять эти действия. Так, например, пункт «Изменение режима контроллера двери» следует выбирать при создании правила для контроллеров с литерой «М»: «КОДОС ЕС-202М» и «КОДОС ЕС-304М».

Для создания нового правила нажмите Новое правило. В окне «Доступные правила» (см. рисунок ниже). При выделении в списке в левой части окна события в правой колонке будет сформирован список действий, определенных при задании связей.

Выбранные событие и действие отображаются внизу окна (Рисунок 3.35).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

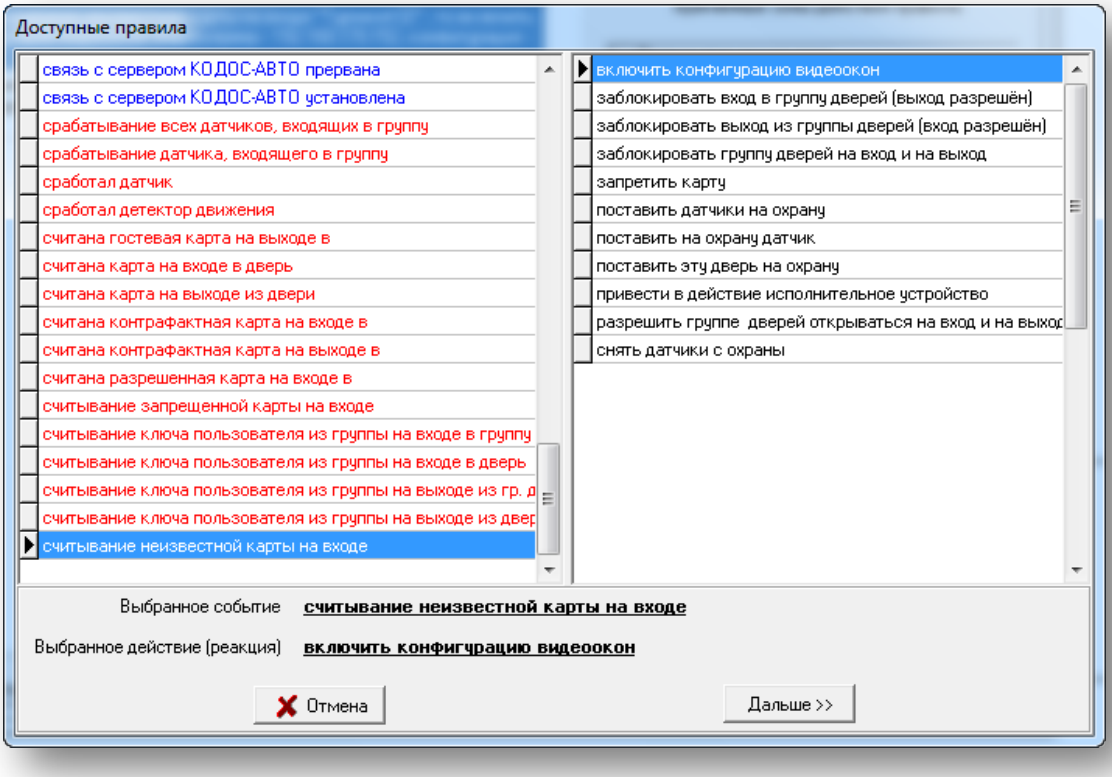


Рисунок 3.35

- Нажмите кнопку «Дальше». В окне «Настройка параметров событий и действий» (Рисунок 3.36) для создаваемого правила запрашиваются вспомогательные параметры его выполнения.

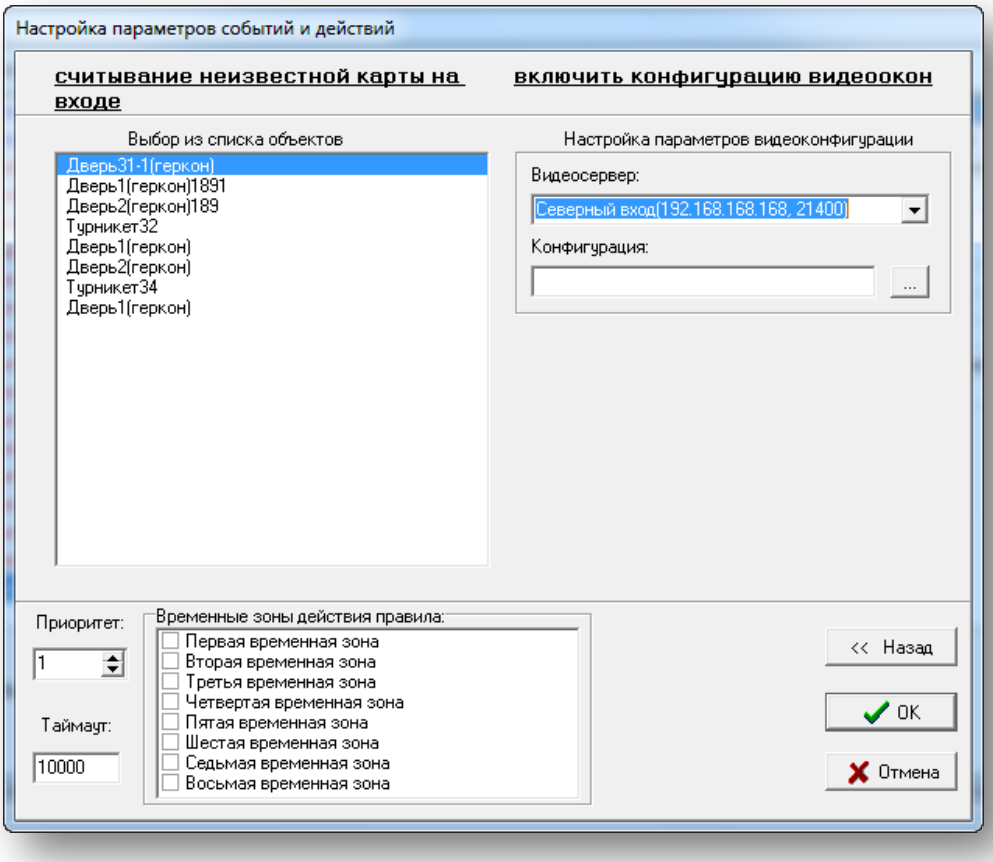


Рисунок 3.36

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Внешний вид окна настройки параметров событий и действий зависит от типа создаваемого правила и позволяет выбрать конкретный объект, пользователя или группу объектов или датчиков. При выборе списка групп будет открыто дополнительно информационное окно с составом данной группы.

Установкой флагов в разделе «Временные зоны действия правила»: (Рисунок 3.36) можно обозначить временные зоны, для которых создаваемое правило будет действовать. Если требуется, чтобы правило действовало все время, следует сбросить все флаги.

Создаваемому правилу может быть присвоен приоритет, определяющий очередность выполнения этого правила. При работе системы в первую очередь выполняются те правила, номер приоритета которых меньше. Для создаваемого правила приоритет задаётся путем ввода числа от 1 до 16 в поле с пошаговым изменением значения «Приоритет».

С помощью поля ввода «Таймаут» может быть задан интервал задержки (в миллисекундах) перед выполнением создаваемого правила. При этом действие, определяемое правилом, будет выполняться спустя заданный интервал от момента возникновения события. Если задержка не нужна, следует установить в этом поле значение 0.

Группа полей ввода «Параметры включения» с пошаговым изменением значения позволяет установить параметры срабатывания устройств.

В поле «Задержка включения» следует установить время (в миллисекундах), которое пройдет, прежде чем устройство сработает.

В поле «Время включения» устанавливается интервал времени (в миллисекундах), в течение которого устройство будет работать.

После настройки всех параметров необходимо сохранить правило в базе данных. Для этого следует нажать кнопку «ОК», расположенную в правом нижнем углу окна. В случае успешного сохранения правила будет выдано соответствующее сообщение.

В окне «Правила» будет выведено сообщение с формулировкой созданного правила (Рисунок 3.37).

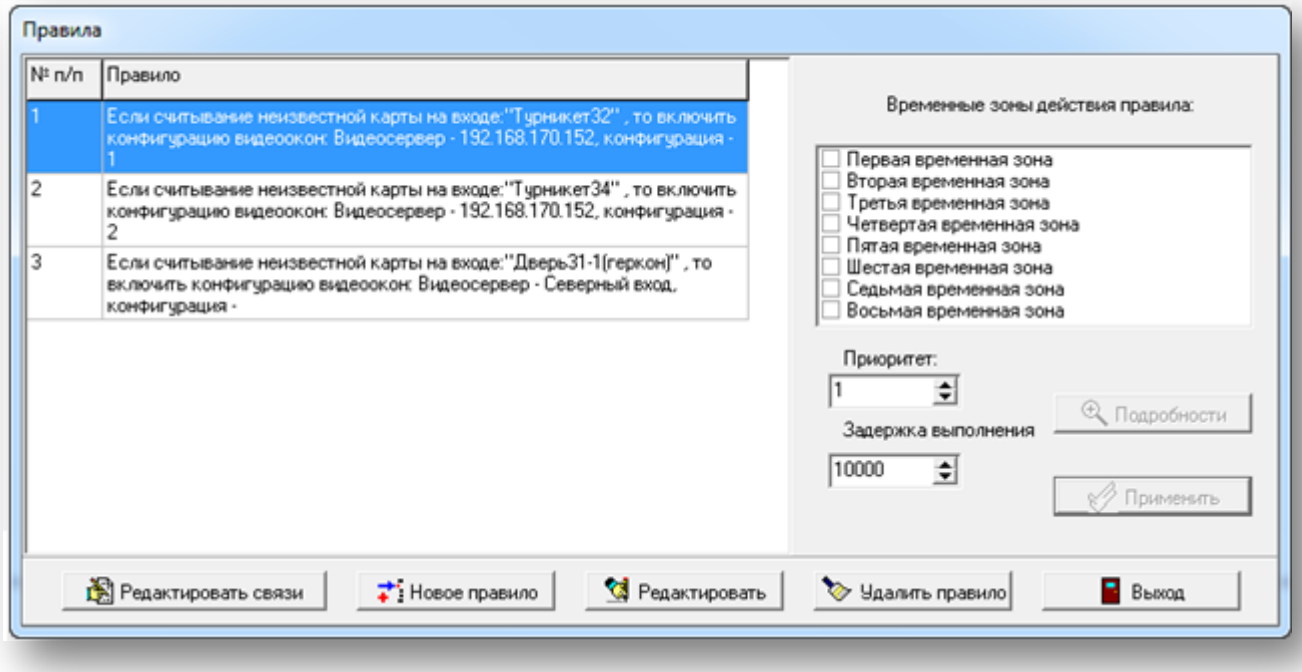


Рисунок 3.37

Для удаления следует нажать кнопку «Удалить правило». Появится окно-запрос подтверждения (Рисунок 3.38).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

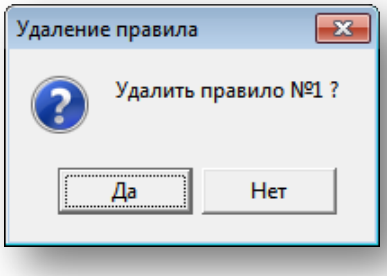


Рисунок 3.38

Далее нажмите «Да» и в окне (Рисунок 3.39) — «ОК».

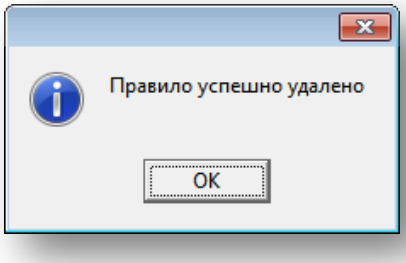


Рисунок 3.39

Если необходимо изменить или ввести новые параметры для создаваемого правила, следует в окне «Правила» (Рисунок 3.37) нажать кнопку «Редактировать». Появится окно «Настройка параметров событий и действий» (Рисунок 3.36), в котором оператор может установить другие параметры.

Выполнение созданных правил происходит автоматически, под управлением программного обеспечения, и не требует дополнительных действий со стороны оператора.

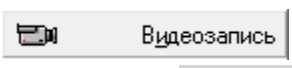
Существует возможность определить период времени, в течение которого программа будет реагировать на произошедшее событие. Если разница во времени между совершенным событием и его приходом на сервер ИКБ превысит установленное значение, то правило выполнено не будет. Это удобно применять, когда выполнение правил нецелесообразно.

Например, при подключении к объекту (ППКОП А-20, контроллер PRO, контроллеры доступа), с которым временно отсутствовала связь, и который определенное время работал в автономном режиме. В этом случае при восстановлении связи происходит «слив событий» — быстрая передача на сервер ИКБ всех накопленных событий, большинство из которых уже потеряла свою актуальность.

Настройка времени выполнения правил проводится в разделе Настройка системы. Значение параметра «Время актуальности события для активации правила» выставляется в секундах и должно быть кратно 60 (при выставлении некратного значения значение округляется в меньшую сторону).

3.14 Настройка видеозаписи

В программе предусмотрена возможность записывать видео при наступлении какого-либо события в системе.

Окно настроек вызывается нажатием кнопки 

в разделе «Управление конфигурацией». В открывшемся окне «Настройка видеокамер» (Рисунок 3.40) .

SEC.RU | Короткий путь к информации
Скачано с sec.ru

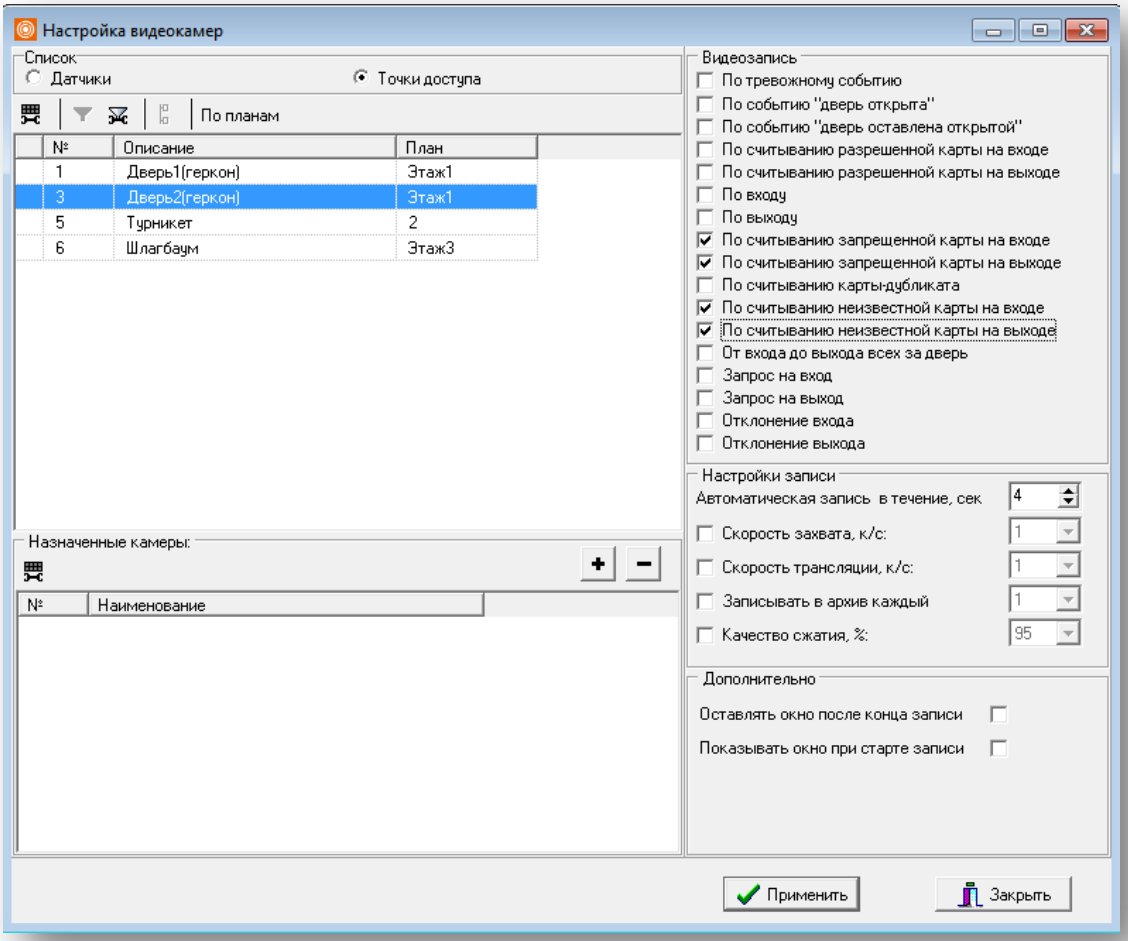


Рисунок 3.40

Раздел «Список»

В разделе представлены все имеющиеся в системе устройства, по событиям от которых может быть записано видео. Изменять вид таблиц в разделе «Список» можно при помощи переключателей «Датчики»/ «Точки доступа» и кнопок в панели инструментов, расположенной в верхней части окна (Рисунок 3.40).

Для сортировки элементов списка, сгруппированных по планам, нажмите кнопку По планам. В противном случае, в списке будут представлены все имеющиеся в системе датчики/ точки доступа.

При нажатии кнопки «По планам» станет активной кнопка , предназначенная для сворачивания или разворачивания представленных в списке групп.

Нажатие кнопки открывает окно «Настройка столбцов» (Рисунок 3.41). Для удобства отображения информации в таблице можно, снимая или устанавливая флаги напротив наименования столбца, включать или исключать его из таблицы. Кроме того, можно изменять расположение столбца в таблице (влево-вправо) при помощи стрелок . Для этого нужно выделить мышью название столбца, а затем стрелками переместить строку. Далее нажмите кнопку «Применить».

SEC.RU | Короткий путь к информации
Скачано с sec.ru

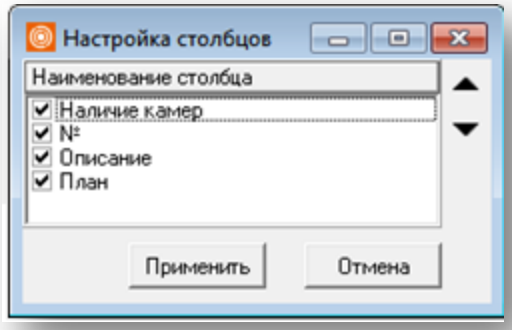


Рисунок 3.41

Нажатие кнопки открывает окно «Настройки фильтра» (Рисунок 3.42), в котором можно задать условия отбора элементов для отображения в списке:

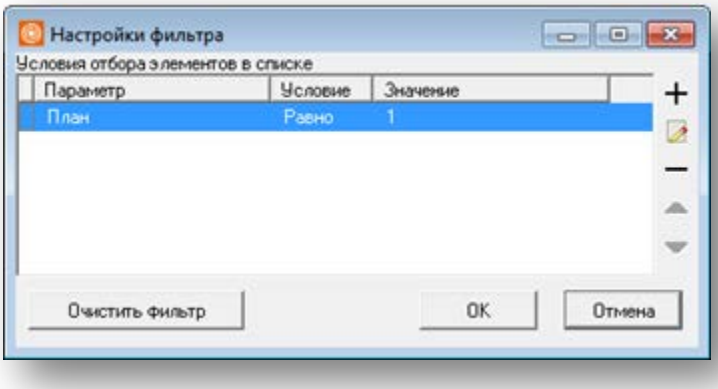


Рисунок 3.42

- Для добавления нового условия нажмите . В открывшемся окне выберите из выпадающих списков параметр (описание или план), условие (равно или не равно) и присвойте значение (см. рисунки ниже).

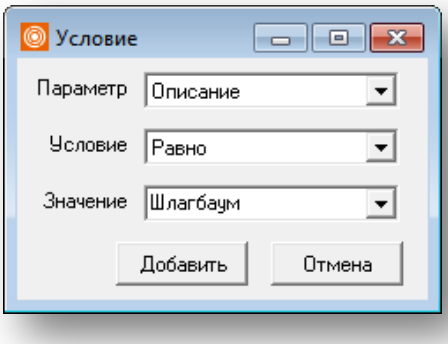


Рисунок 3.43

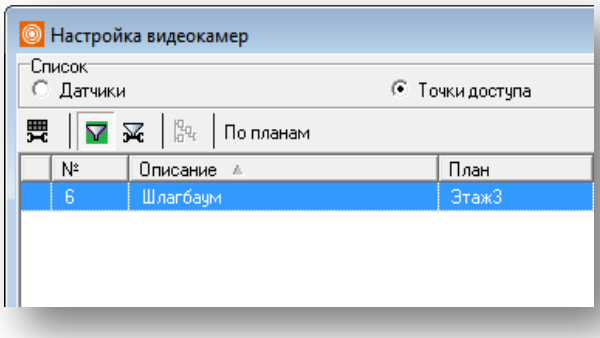


Рисунок 3.44

Нажмите «Добавить», «ОК», а затем кнопку включения/ выключения фильтра . Состав строк в списке окна «Настройка видеокамер» будет изменен в соответствии с заданным критерием (Рисунок 3.43).

Если в качестве условия выбрать «Не равно», для отображения в списке будут выбраны элементы, параметры которых не будут соответствовать введенному значению. Пример приведен на рисунках ниже.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

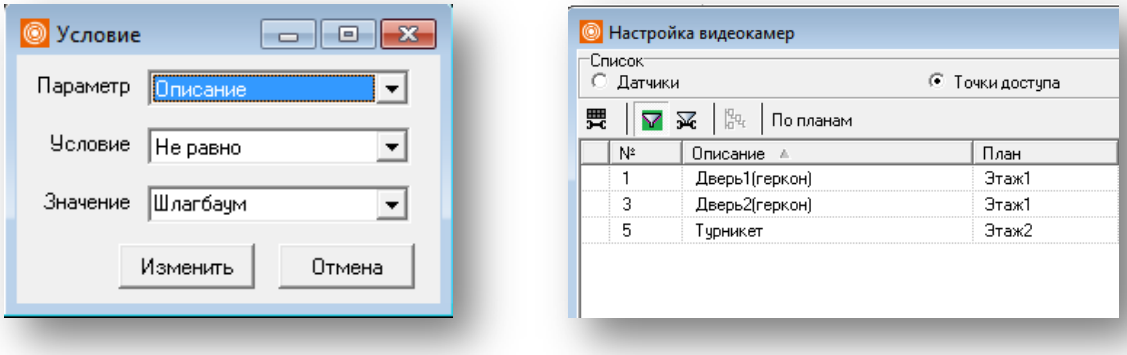
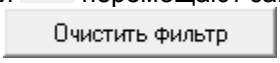


Рисунок 3.45

Для редактирования условий отбора элементов в окне «Настройки фильтра» (Рисунок 3.42) выделите строку с условием, которое нужно изменить, нажмите кнопку  и внесите необходимые коррективы. Затем нажмите кнопку «Изменить» (см. рисунок выше) и «ОК».

В случае если список точек доступа/ датчиков, по событиям от которых будет записываться видео, объемный и поиск нужных записей представляется затруднительным, рекомендуется в окне «Настройки фильтра» (Рисунок 3.42) создать несколько условий с разными параметрами для более точного поиска.

- Нажатие кнопки удаляет выделенное условие.
- Стрелки  перемещают запись с условием вверх или вниз.
- Кнопка  удаляет все условия.

Раздел «Назначенные камеры»

Выберите точку доступа или датчик в разделе «Список», затем в разделе «Назначенные камеры» нажмите . В открывшемся окне «Добавление видеокамер» (Рисунок 3.46) выберите камеру или несколько (при помощи Ctrl или Shift), затем нажмите кнопку «Выбор».

Нажатие кнопки  открывает окно «Настройка столбцов» (описание для рисунка 4.33 см. выше).

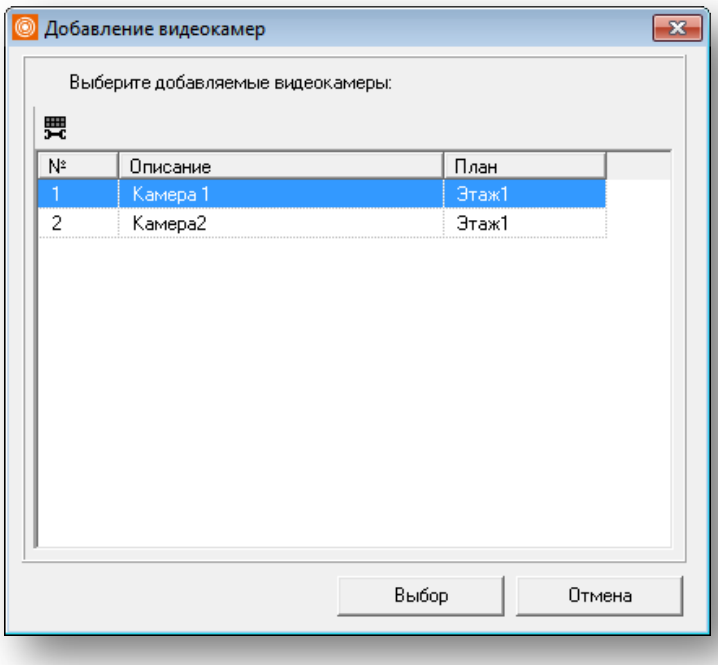


Рисунок 3.46

SEC.RU | Короткий путь к информации
Скачано с sec.ru

В разделе «Назначенные камеры» появится запись (см. рисунок ниже).

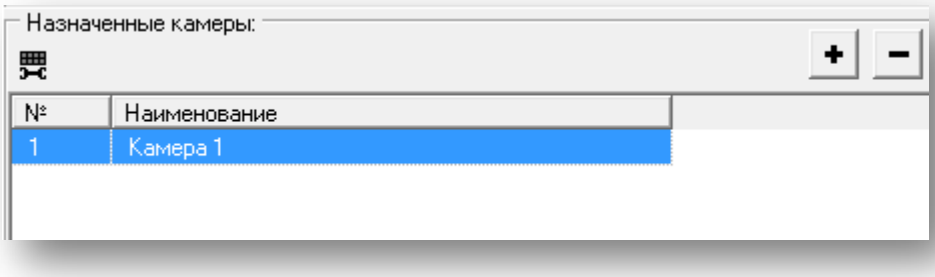


Рисунок 3.47

Далее нажмите кнопку «Применить» в окне «Настройка видеокамер» и значок камеры появится в таблице раздела «Список» напротив выбранной точки доступа или датчика (Рисунок 3.48).

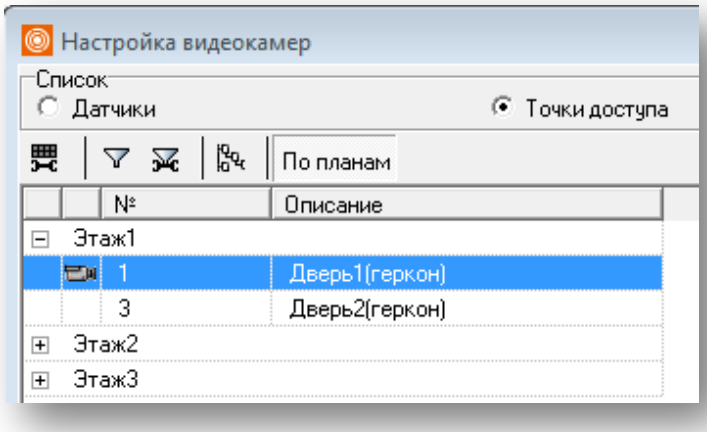


Рисунок 3.48

Кнопка − удаляет выделенную камеру.

В разделе «Видеозапись» необходимо отметить флагом событие, по которому будет проводиться видеозапись. Список событий меняется в зависимости от выбранного датчика.

В разделе «Настройки записи» значения параметров «Скорость захвата», «Качество сжатия», «Автоматическая запись в течение», «Скорость трансляции», «Записывать в архив каждый» выставляются по необходимости.

Раздел «Дополнительно»

Для вывода видеоокна на экран при наступлении события отметьте значение «Показывать окно при старте записи». При выставлении значения «Оставлять окно после конца записи» окно видеоизображения останется на экране. В дальнейшем его можно будет закрыть вручную.

ПРИМЕЧАНИЕ – Также, можно настроить запись видео (установить поворотное устройство видеокамеры на определенную позицию) в ответ на какое-либо событие в системе, используя настройки правил (подробнее в разделе Настройка правил).

3.15 Настройка интегрированного видео

В зависимости от способа получения видеоизображения для использования видео в составе ИКБ «КОДОС» необходимо иметь соответствующие лицензии:

Если видеоизображение получают с сервера «Globoss», «КОДОС-Авто» или «КОДОС-Видеосеть», в списке лицензий должно быть указано: «интегрированное видео базовая лицензия (все функции СКД, связанные с видео)». Эта лицензия предоставляется бесплатно.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Если видеоизображение получают от плат видеозахвата, а также USB-камер, подключенных к компьютеру — серверу или клиенту ИКБ, в списке лицензий должны быть:

- «КодосВидео базовая лицензия (все функции СКД, связанные с видео)»;
- «N источников видео для СКД»;
- «N каналов передачи звука».

После настройки видеоинформация становится доступной для компьютеров в составе системы. Ограничения по доступу и управлению видеоисточниками для каждого компьютера устанавливаются индивидуально.

Источники видео могут быть сетевые и интегрированные.

ПРИМЕЧАНИЕ – Подробнее о добавлении и редактировании свойств сетевых и интегрированных видеоисточников, а также о настройке поворотных устройств см. «Руководство оператора программы „Конфигуратор“».

3.16 Управление поворотным устройством

Запустите программу «Сервер ИКБ» или клиентское приложение, введите имя оператора и пароль, затем перейдите во вкладку «Планы», далее — «Этаж».

Щелчком правой кнопки мыши по иконке видео на плане вызвать контекстное меню и выбрать «Поворотное устройство». При установлении связи вкладка «Управление» станет активной, и появится окно с кнопками управления поворотным устройством (Рисунок 3.49).

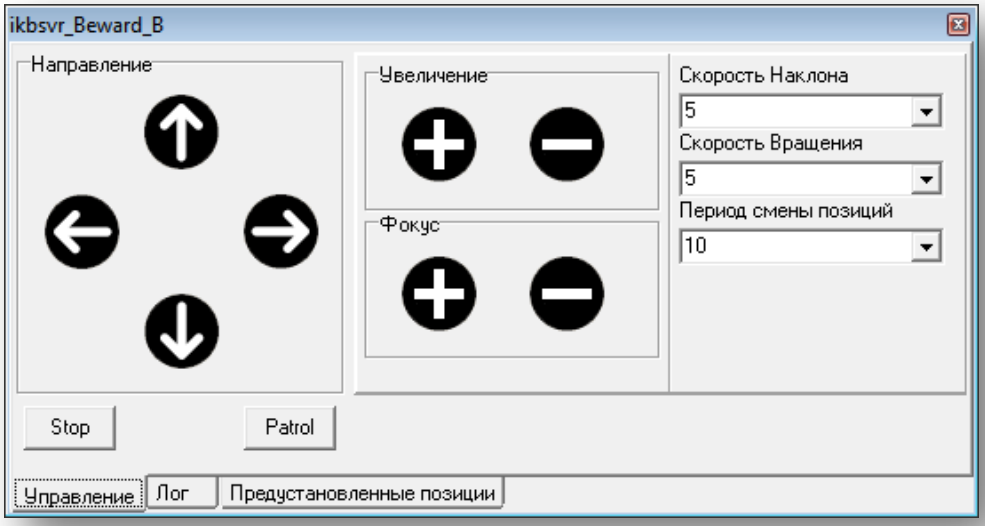


Рисунок 3.49

Вкладка «Управление»

- Раздел «Направление» содержит кнопки для управления устройством по вертикали, горизонтали и фиксация камеры в центре кадра.
- Раздел «Увеличение» содержит кнопки увеличения и уменьшения изображения.
- Раздел «Фокус» содержит кнопки управления фокусом.
- «Скорость Наклона» — выпадающий список, предназначенный для управления скоростью перемещения камеры по вертикали в относительных единицах.
- «Скорость Вращения» — выпадающий список, предназначенный для управления скоростью перемещения камеры по горизонтали в относительных единицах.
- «Период смены позиций» — выпадающий список, позволяющий регулировать время остановки камеры в каждой позиции при патрулировании.
- Нажатие кнопки «Stop» — прекращает автоматическое движение камеры при патрулировании.
- Нажатие кнопки «Patrol» — перемещает камеру по заданным пользователем координатам.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Вкладка «Лог»

Во вкладке отображается список и фиксируется время каждого события (Рисунок 3.50). Если подключение к поворотному устройству отсутствует, то вкладка «Лог» станет активной и появится соответствующее сообщение.

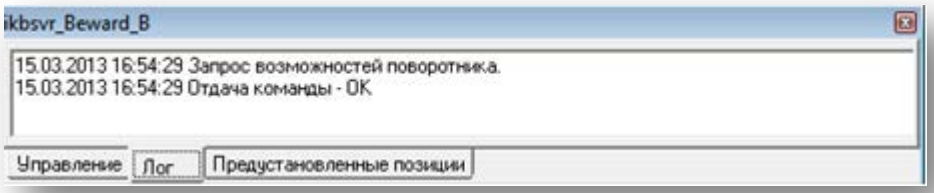


Рисунок 3.50

Вкладка «Предустановленные позиции»

Во вкладке «Предустановленные позиции» пользователь устанавливает точки патрулирования и задаёт им имена.

Для добавления позиции в список патрулирования следует, используя кнопки управления камерой во вкладке «Управление», установить камеру в нужное положение.

Далее во вкладке «Предустановленные позиции», в поле «Текущая позиция» следует задать ее имя и нажать кнопку «Запомнить». Поворотное устройство будет перемещаться по координатам в порядке их добавления в память (Рисунок 3.51).

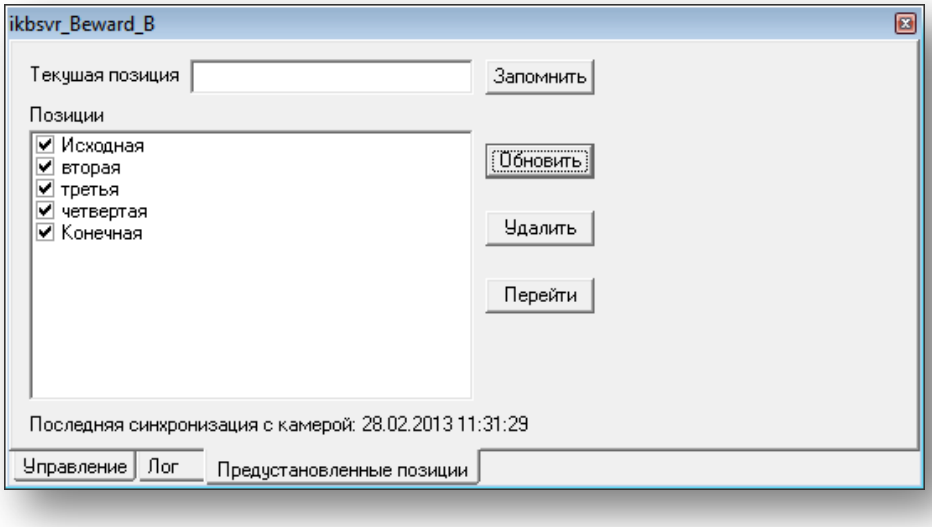


Рисунок 3.51

Для просмотра списка заданных точек патрулирования следует нажать кнопку «Обновить» и в списке «Позиции» будут указаны все точки патрулирования, расположенные в порядке добавления. Для проверки сохраненной позиции необходимо выделить ее и нажать кнопку «Перейти» — камера переместится в указанную позицию. Кнопка «Удалить» удаляет выбранную позицию.

Для исключения из списка патрулирования некоторых позиций следует во вкладке «Предустановленные позиции» снять флажки напротив выбранных точек (Рисунок 3.52).

SEC.RU | Короткий путь к информации Скачано с sec.ru

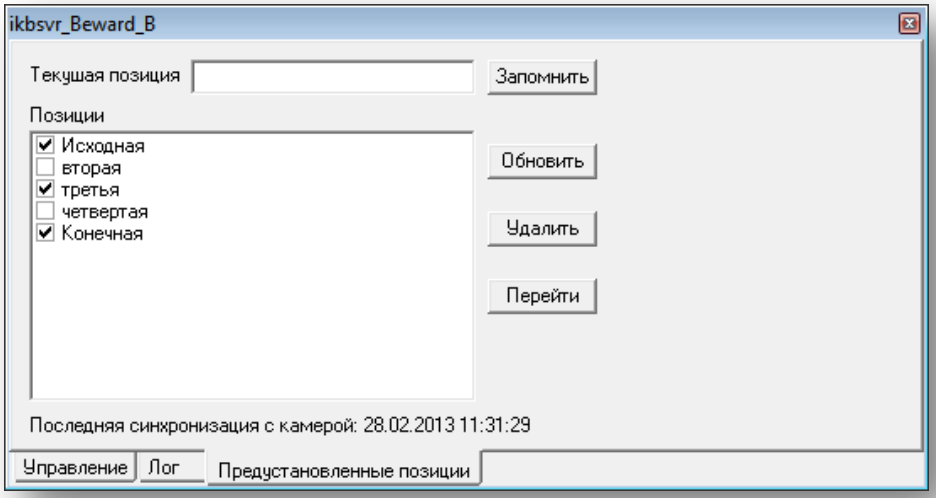


Рисунок 3.52

Для просмотра видео необходимо навести курсор мыши на ярлык видеокамеры на плане и одинарным щелчком левой кнопки мыши включить просмотр (Рисунок 3.53).

ПРИМЕЧАНИЕ – Каждому оператору присваивается определенный набор прав, в том числе связанный и с возможностью управлять видеонастройками. В зависимости от этих настроек для разных операторов внешний вид окна управления видео может различаться — могут быть недоступны определенные функции и, в соответствии с этим, не будут отображаться некоторые кнопки на панели управления. Подробнее о настройке прав оператора см. Назначение прав операторам.



Рисунок 3.53

На панели инструментов окна имеются кнопки записи и управления видеоизображением:

-  «Начать запись» — нажатие кнопки включает запись видео.
-  «Остановить запись» — нажатие кнопки останавливает запись видео.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- «Показать архив» — при нажатии на кнопку появляется окно просмотра и управления видеоархивом (Рисунок 3.54).
- «Увеличить видеоокно в 2 раза» — при нажатии кнопки окно видео будет увеличено в два раза.
- «Уменьшить видеоокно в 2 раза» — при нажатии кнопки окно видео будет уменьшено в 2 раза.

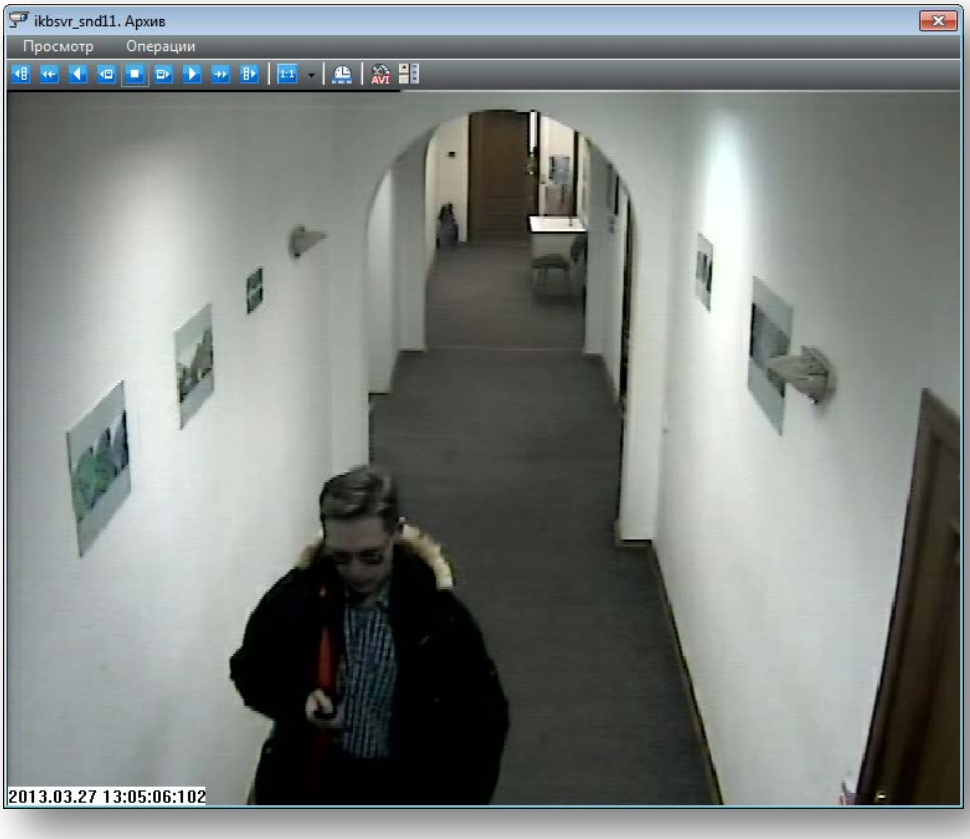


Рисунок 3.54

Элементы главного меню окна «Архив»

1) Просмотр

Элемент «Просмотр» главного меню окна «Архив» (Рисунок 3.54) содержит список возможных способов навигации по видеоархиву. Для удобства они продублированы в панели инструментов.

- «Предыдущая запись» — нажатием на кнопку выполняется переход к предыдущему фрагменту записи в видеоархиве.
- «Ускоренная перемотка назад» — ускоренное воспроизведение видеозаписи назад.
- «Обратное воспроизведение» — при нажатии на кнопку видеозапись будет воспроизводиться в обратном порядке.
- «Кадр назад» — демонстрация предыдущего кадра просматриваемой видеозаписи.
- «Стоп» — нажатие кнопки останавливает просмотр видеоархива.
- «Кадр вперед» — демонстрация последующего кадра просматриваемой видеозаписи.
- «Воспроизведение» — кнопка включения просмотра видеозаписи.
- «Ускоренная перемотка вперед» — воспроизведение видеозаписи в ускоренном режиме.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

-  «Следующая запись» — нажатием на кнопку осуществляется переход к последующей по порядку записи в видеоархиве.
-  «Скорость перемотки» — выбор скоростного режима перемотки видеозаписи. Одинарным щелчком левой кнопки мыши по выпадающему списку выбрать режим перемотки (Рисунок 3.55).

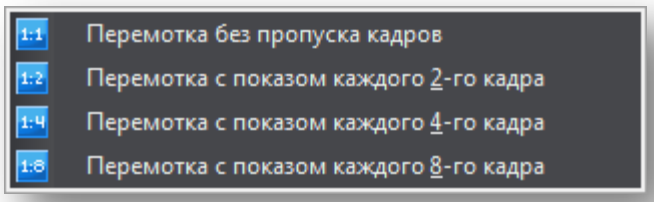


Рисунок 3.55

2) Операции

При выборе элемента «Операции» в главном меню окна «Архив» (Рисунок 3.54) появится список команд для управления. Они также продублированы в панели инструментов.

- Позиционировать по времени. При нажатии откроется окно, где можно выбрать необходимое время для просмотра записи архива (Рисунок 3.56).

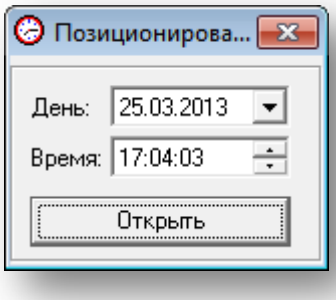


Рисунок 3.56

- «Записать кадр в файл» — при нажатии на кнопку кадр будет сохранен в указанную папку в формате .jpg (Рисунок 3.57).

SEC.RU | Короткий путь к информации Скачано с sec.ru

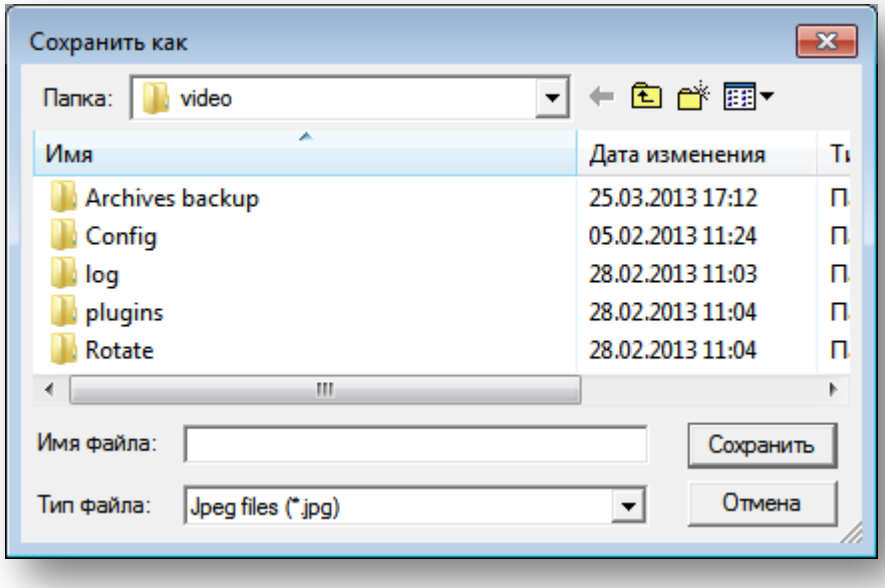


Рисунок 3.57

- «Распечатать кадр» — при нажатии на кнопку появится окно управления печатью (Рисунок 3.58).

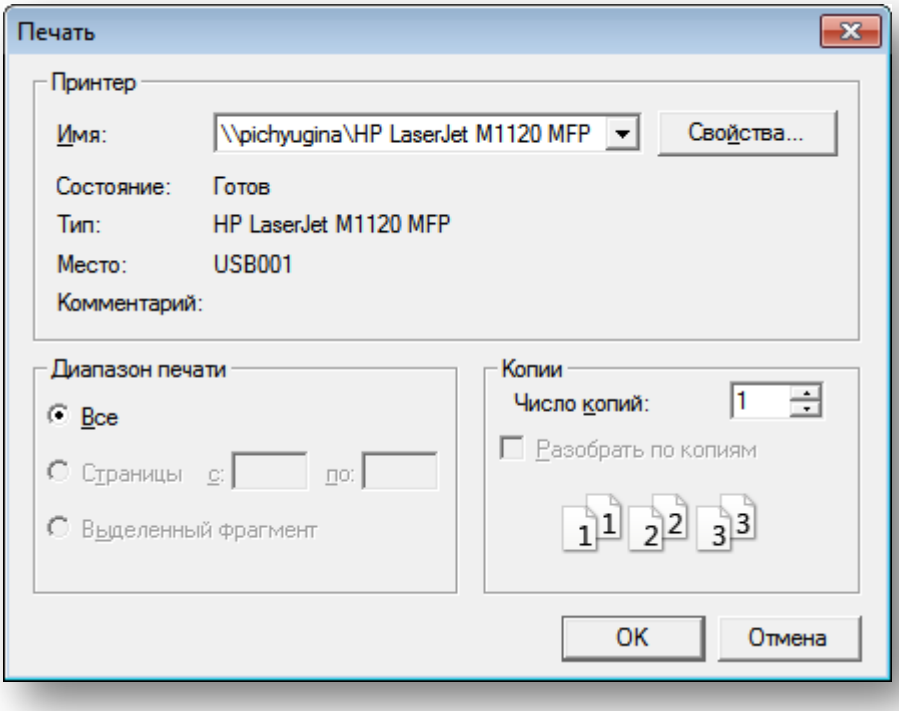


Рисунок 3.58

- «Запись фрагмента архива в AVI» — при нажатии на кнопку появится окно «Запись архива в AVI» (Рисунок 3.59).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

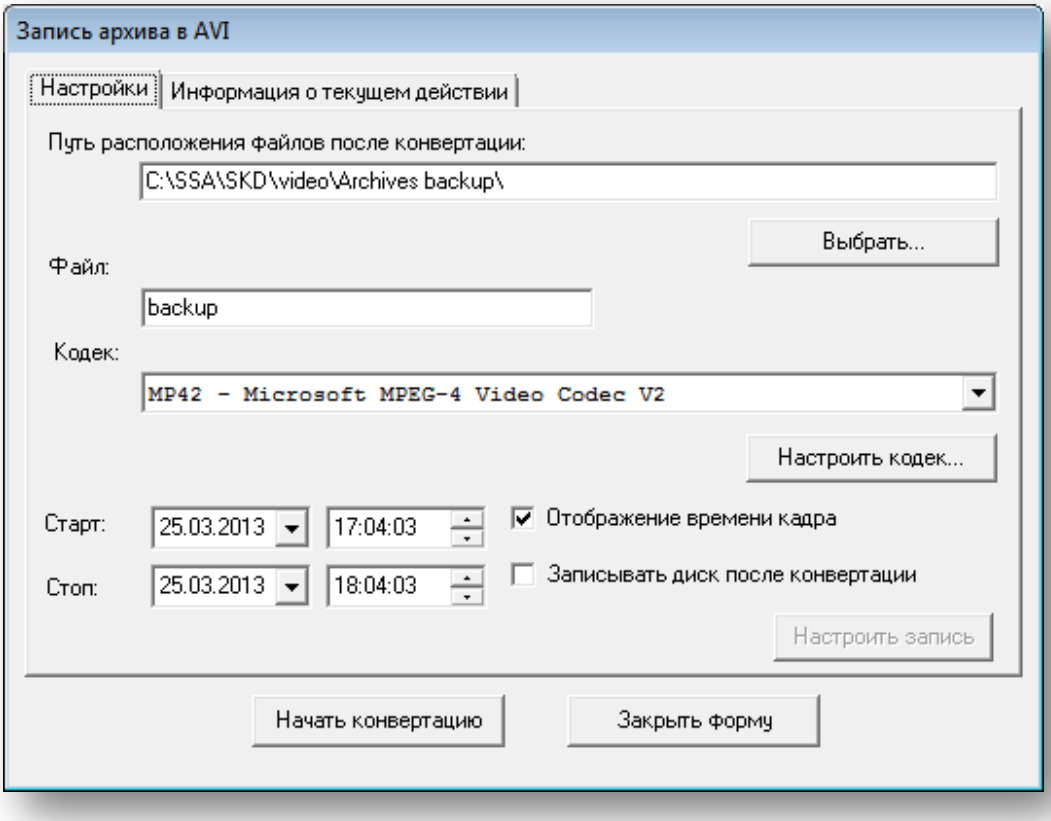


Рисунок 3.59

- «Бегунок по архиву» — навигация по архиву (выбор фрагмента видеозаписи для просмотра) может осуществляться также перемещением «бегунка» (Рисунок 3.60).

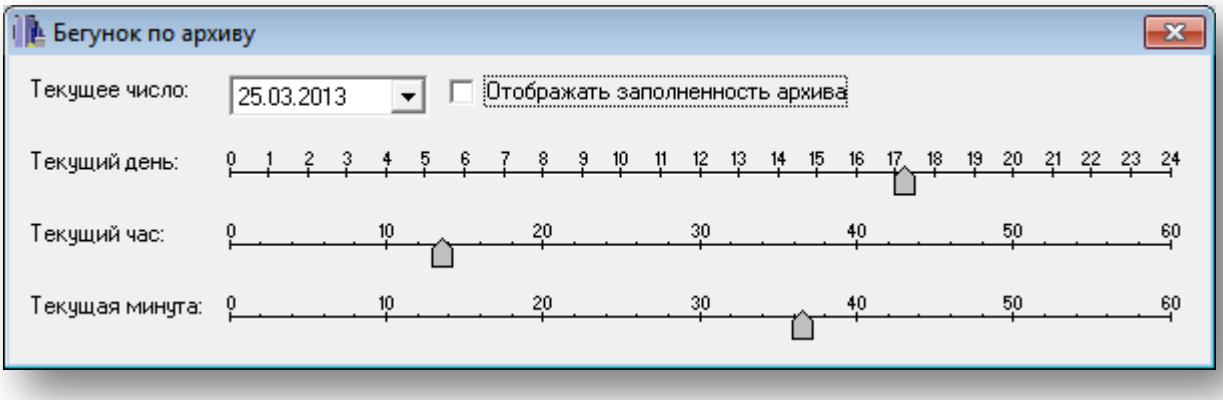


Рисунок 3.60

Если опция «Отображать заполненность архива» отмечена флагом, то ярко-зеленым цветом будут выделены временные отрезки, в которые проводилась видеозапись (Рисунок 3.61).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

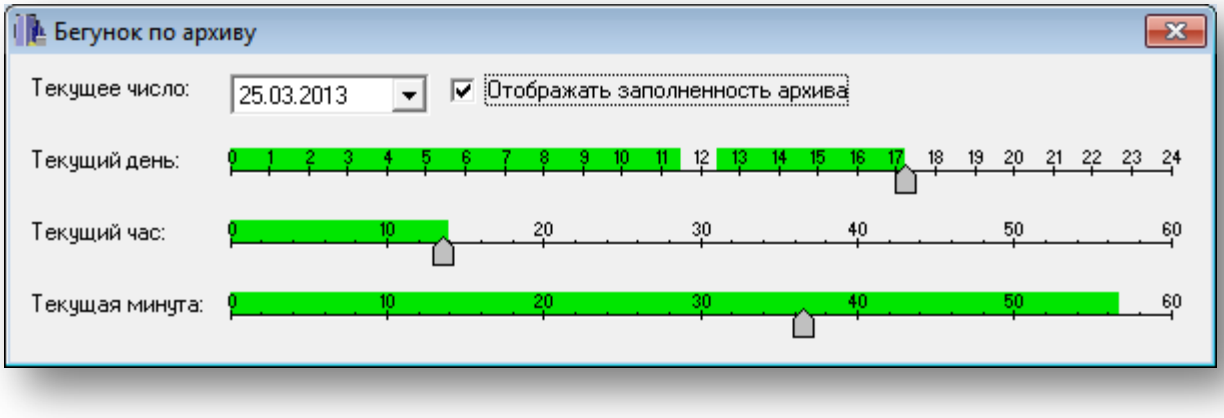


Рисунок 3.61

3.17 Мультиконфигурации

Режим «Мультиконфигурации» предназначен для быстрого переключения сетевых видеоканалов клиентского приложения Globoss между различными видеоисточниками без перезагрузки самих видеоканалов. Переключение происходит по команде от сервера ИКБ, которая содержит имя целевой мультиконфигурации.

- Настройки мультиконфигурации следует прописать в файле multiconfig.ini, который находится в корневой папке установленного клиентского приложения Globoss: D → SSA →GLOBOSS → multiconfig.ini. Файл multiconfig.ini открывается текстовым редактором «Блокнот». Вид файла представлен в левой колонке в таблице ниже:

SEC.RU | Короткий путь к информации Скачано с sec.ru

Вид файла	Назначение строк
[**Проходная**] **panel_conf=4x4** **channel_1=**192.168.1.1:КПП_улица **channel_2=**192.168.1.1:Турникет **channel_3=**192.168.1.1:Пульт_охраны **channel_4=**192.168.1.1:Шлагбаум **[Офис_1_этаж]** **channel_1=**192.168.1.2:Вход_с_улицы **channel_2=**192.168.1.2:Запасный_выход **channel_3=**192.168.1.2:Вестибюль **channel_4=**192.168.1.2:Пульт_охраны **channel_5=**192.168.1.2:Ресепшн **channel_6=**192.168.1.2:Лестница **[Тревога]** **panel_conf=3x2** **channel_1=**192.168.1.1:Пульт_охраны **channel_2=**192.168.1.1:КПП_улица **channel_3=**192.168.1.2:Пульт_охраны **channel_4=**192.168.1.2:Вход_с_улицы **channel_5=**192.168.1.2:Вестибюль **channel_6=**192.168.1.2:Ресепшн	[Имя_мультиконфигурации] panel_conf=<имя конфигурации видеоокон> channel_<номер>=<ip-адрес сервера>:<имя канала на сервере>

- Имя мультиконфигурации — имя, которое передаётся по запросу ИКБ. Видеоканалы Globoss будут переключены на те, которые включены в состав данной мультиконфигурации.

ВНИМАНИЕ! Имя мультиконфигурации не должно совпадать с именем какой-либо конфигурации каналов на клиенте Globoss.

- Имя конфигурации видеоокон — формат расположения видеоокон в окне клиентского приложения Globoss, который будет выведен на монитор при переключении на заданную мультиконфигурацию.
- channel_<номер> — порядковый номер видеоканала в программе Globoss (от 1 до 64), к которому будут применены данные настройки.
- IP-адрес сервера — адрес сервера, который будет назначен данному видеоканалу.
- Имя канала на сервере — имя видеоисточника на сервере Globoss, который будет назначен данному видеоканалу.

ПРИМЕЧАНИЕ –
Количество мультиконфигураций не ограничено.
Допускается от 1 до 4 каналов в мультиконфигурации.
Допускается отсутствие привязки мультиконфигурации к конфигурации расположения видеоокон.

Запуск клиентского приложения Globoss в режиме мультиконфигураций осуществляется с указанием ключа/ multiclient<количество каналов>, где параметр <количество каналов> задает максимальное количество видеоканалов, которые клиентское приложение Globoss будет использовать для мультиконфигураций.

Пример настройки мультиконфигурации

- Во вкладке «Управление» нажмите кнопку «Видеоисточники». В открывшемся окне «Настройка списка видеосерверов» (Рисунок 3.62) необходимо добавить объекты — настройки для подключения к АРМ «Globoss».
- Нажмите кнопку «Добавить» (Рисунок 3.62).

SEC.RU | Короткий путь к информации Скачано с sec.ru

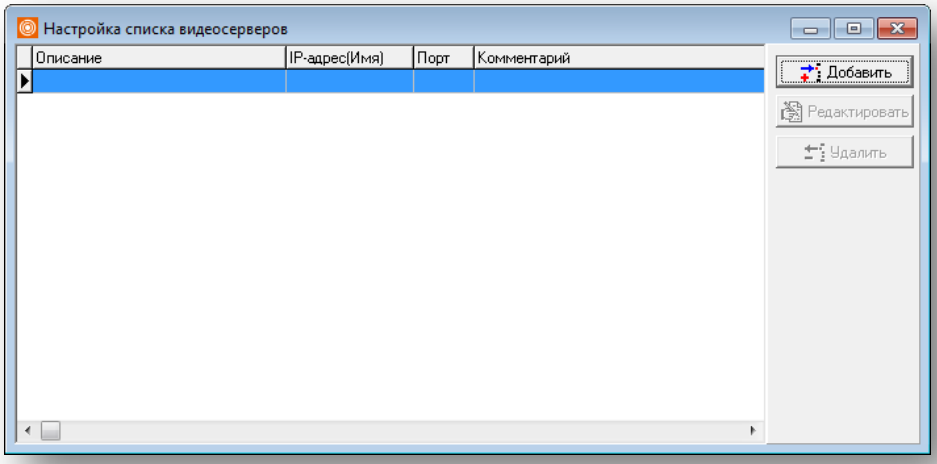


Рисунок 3.62

- В окне «Добавление нового сервера» (Рисунок 3.63) введите описание (может быть произвольным), порт и IP-адрес компьютера с установленным АРМ Globoss. Номер порта необходимо узнать у администратора системы видеонаблюдения Globoss.

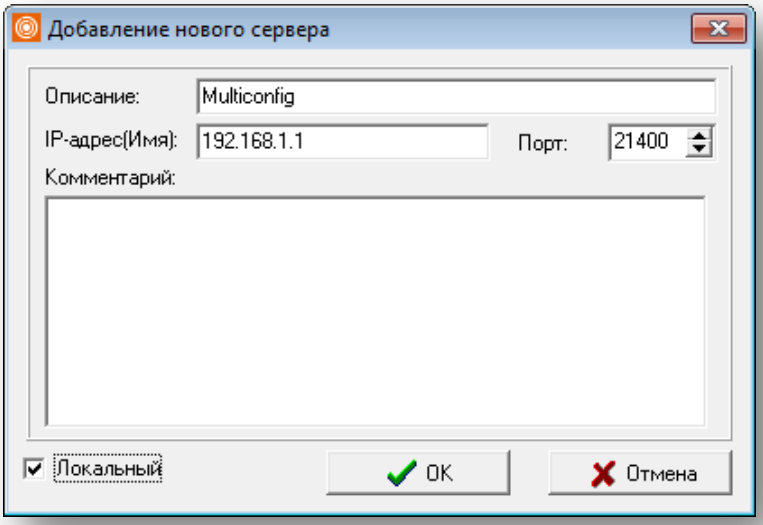


Рисунок 3.63

«Локальный» — это настройка для текущего рабочего места ИКБ. Флаг устанавливают при добавлении ПК – клиента Globoss, которому требуется настроить смену конфигурации видеоокон «по нажатию». Так, при нажатии по значку датчика во вкладке «Планы» конфигурация видеоокон будет менятся только на тех видеоисточниках (сервере или клиентах Globoss), для которых на данном АРМ ИКБ установлен параметр «Локальный»; видеоархивы из окна тревожных событий также будут открываться только на том клиенте Globoss, для которого был установлен флаг «Локальный».

- Нажмите «ОК». Видеосервер внесен в список (Рисунок 3.64).

SEC.RU | Короткий путь к информации Скачано с sec.ru

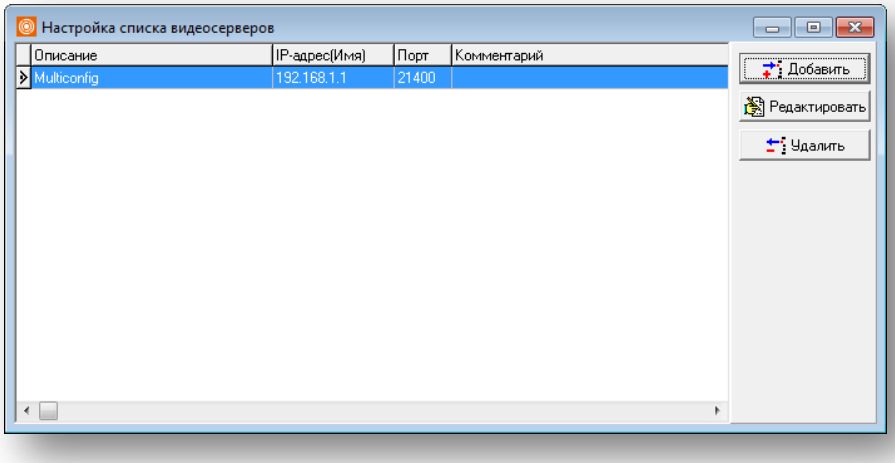


Рисунок 3.64

- Закройте окно. Нажмите кнопку «Конфигурация видео» во вкладке «Управление». В окне «Редактирование конфигурации видео» для удобства просмотра элементов списка можно сгруппировать их по планам. Для этого нажмите кнопку По планам (Рисунок 3.65).

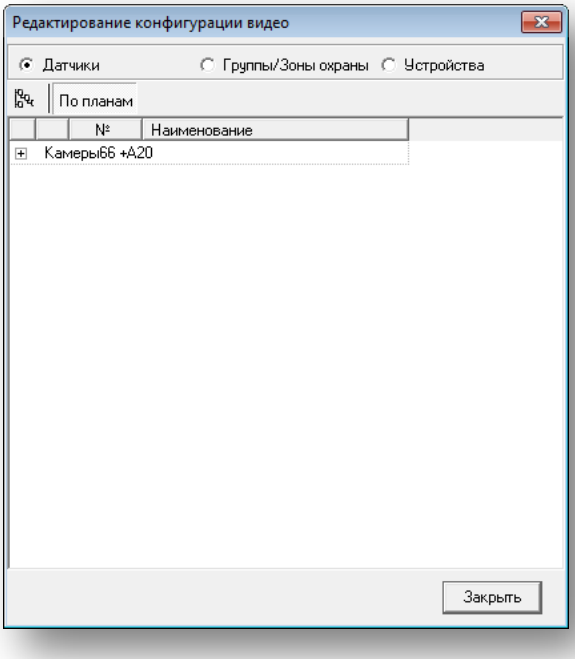


Рисунок 3.65

- При нажатии кнопки «По планам» станет активной кнопка , предназначенная для сворачивания или разворачивания представленных в списке групп. При нажатии кнопки в списке будут представлены все имеющиеся в системе датчики/ группы/ зоны охраны/ устройства, в зависимости от выбранного типа сортировки элементов списка (Рисунок 3.66).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

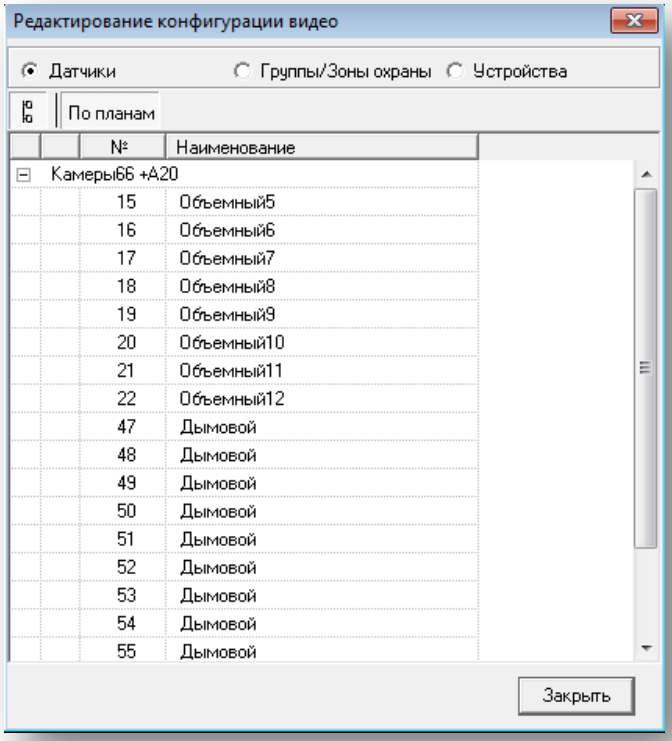


Рисунок 3.66

- Двойным щелчком по элементу откройте окно «Привязка конфигурации видео» (Рисунок 3.67).

ПРИМЕЧАНИЕ – Содержание этого окна для групп, устройств и для датчиков будет различаться.

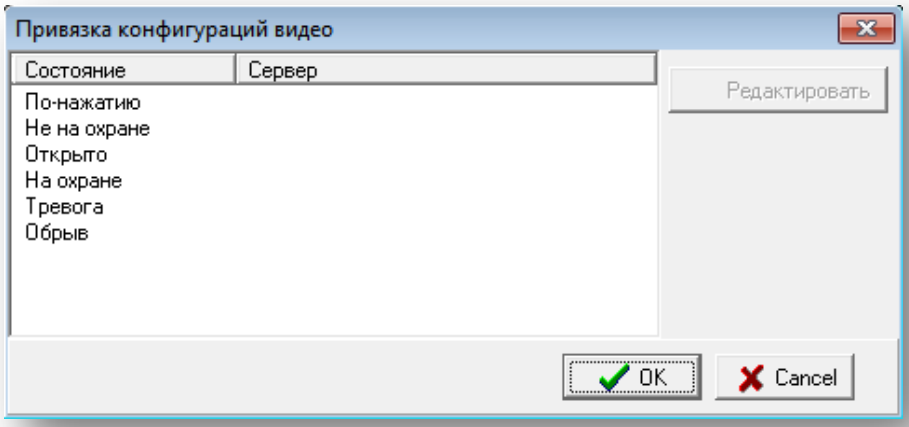


Рисунок 3.67

- Выберите состояние датчика/ группы/ зоны охраны/ устройства, к которому привязывается конфигурация видео. Например, выбираем состояние «По нажатию» для Двери 1. Затем — «Редактировать» (кнопка станет активной).

SEC.RU | Короткий путь к информации Скачано с sec.ru

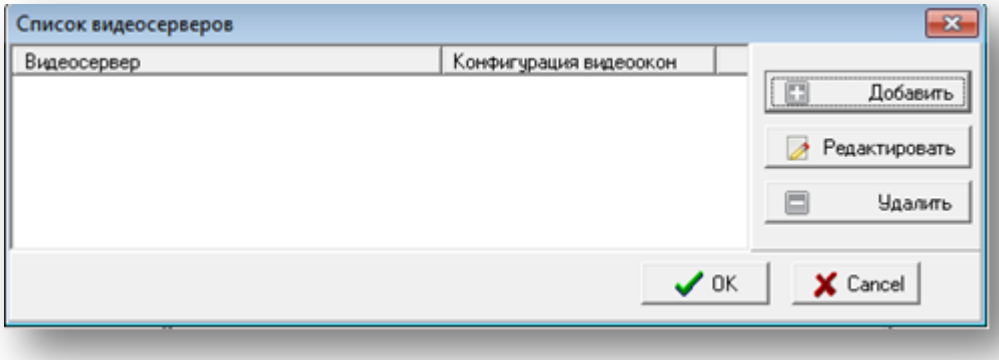


Рисунок 3.68

- В окне «Список видеосерверов» нажмите кнопку «Добавить» (Рисунок 3.68).

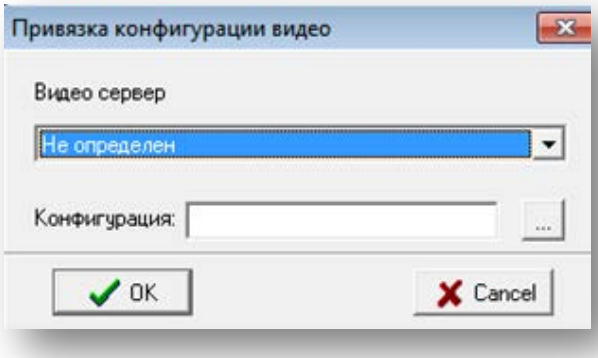


Рисунок 3.69

- В открывшемся окне «Привязка конфигурации видео» (Рисунок 3.69) из выпадающего списка выберите видеосервер. Напротив поля «Конфигурации» нажмите кнопку ....

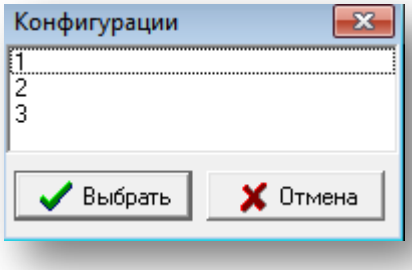


Рисунок 3.70

- В открывшемся окне «Конфигурации» (Рисунок 3.70) укажите в списке нужную конфигурацию камер (опирайтесь на сведения, содержащиеся в файле multiconfig.ini). Затем нажмите кнопку «Выбрать».
- В окне «Привязка конфигурации к видео» появится выбранная конфигурация. В нашем примере — 1.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

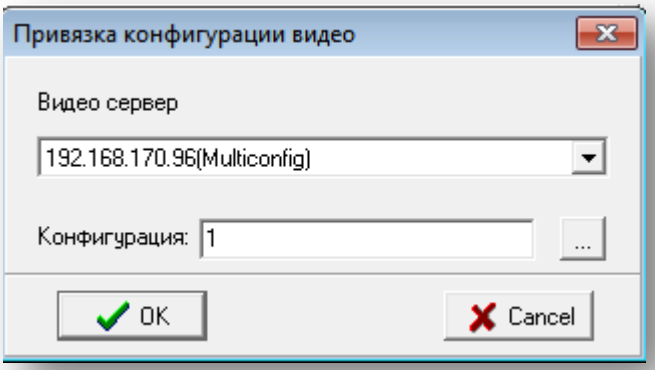


Рисунок 3.71

- Нажмите «ОК». В окне «Список видеосерверов» (Рисунок 3.72) появится выбранная конфигурация.

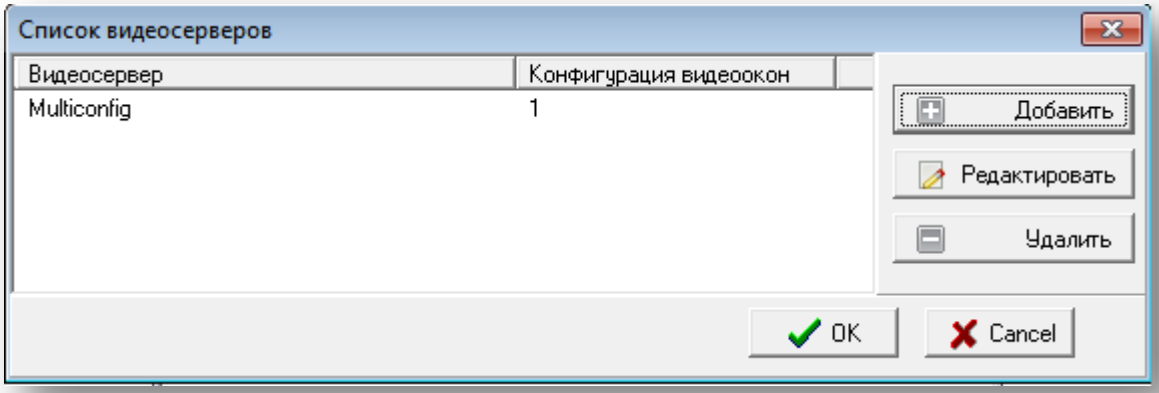


Рисунок 3.72

- Нажмите «ОК». В окне «Привязка конфигураций видео» в поле «Сервер» будет указан IP-адрес компьютера – АРМ Globoss и номер выбранной конфигурации.

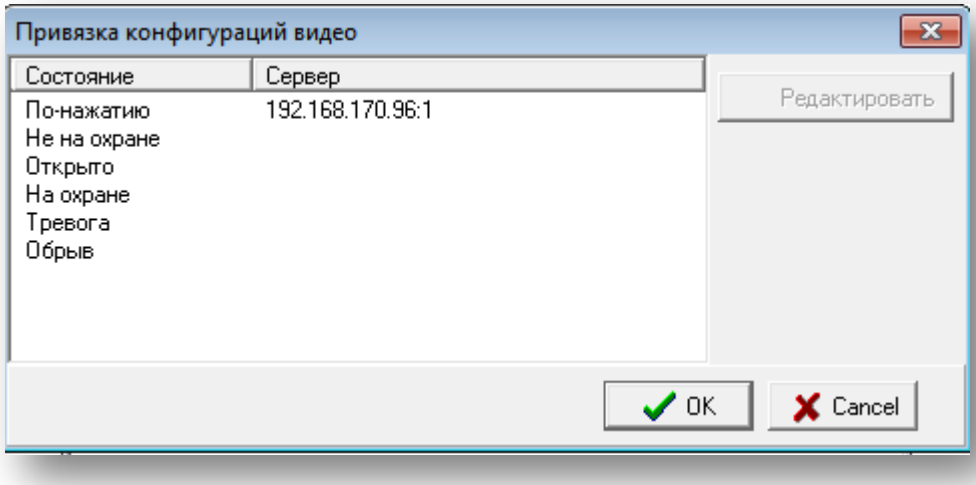


Рисунок 3.73

- Для завершения настроек нажмите «ОК».

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.18 Настройка режима запрета повторного прохода

Режим запрета повторного прохода (далее ЗПП) не даёт пользователю пройти через и одну и ту же точку доступа (дверь, турникет) более одного раза подряд в одном направлении. Для корректной работы режима необходима установка на всех точках доступа считывателей с двух сторон (на «вход» и на «выход»).

При проходе в дверь, оборудованную считывателем, следует «отмечаться» на вход и на выход. Факт прохода определяется поднесением ключа к считывателю и открытием двери (если дверь уже открыта, достаточно поднести кодоноситель к считывателю и факт прохода будет зафиксирован системой). В случае повторного прохода (например, если Вы отметились при входе, а при выходе нет, и снова пытаетесь войти) дверь будет заблокирована, а считыватель будет мигать поочередно красно-зеленым светом, информируя о попытке повторного прохода.

Режим ЗПП может быть глобальным и локальным. Локальный контролирует ЗПП только на одной точке доступа. Если ЗПП необходим на нескольких точках доступа одновременно (например, в большом помещении с несколькими дверями, этаж здания и т. п.), необходимо настраивать контур и включать в него точки доступа (при этом не должно быть других способов проникнуть в пределы контура), ограничивающие проход в него.

3.18.1 Настройка глобального ЗПП

Для настройки контура, в рамках которого действует режим запрета повторного прохода, во вкладке «Управление», в разделе «Управление конфигурацией» нажмите кнопку 

.

- В открывшемся окне «Настройка контуров контроля повторного прохода» (Рисунок 3.74) нажмите кнопку  «Новый контур» и задайте ему имя.

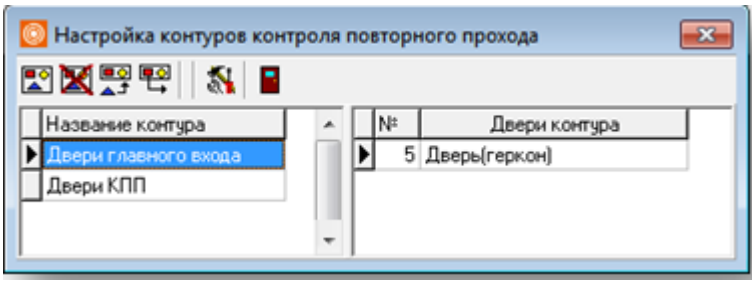


Рисунок 3.74

- Затем нажмите кнопку  «Добавить в контур» и выберите двери, подлежащие включению в него. Далее — «ОК» (Рисунок 3.75).

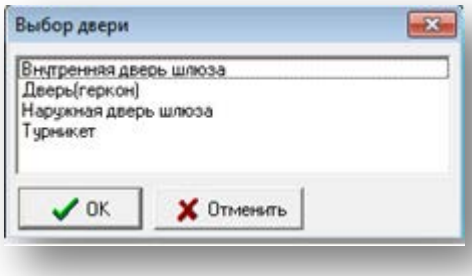


Рисунок 3.75

- Для удаления из контура ЗПП какой-либо двери, выделите ее название в списке и нажмите в окне «Настройка контуров контроля запрета повторного прохода» (Рисунок 3.74) кнопку  «Удалить из контура». В окне с предупреждением (Рисунок 3.76) нажмите «Да».

SEC.RU | Короткий путь к информации
Скачано с sec.ru

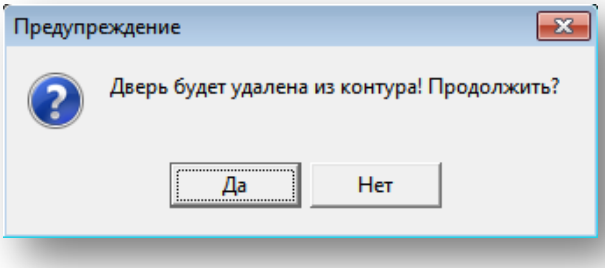


Рисунок 3.76

3.18.2 Настройка локального ЗПП

Для настройки локального ЗПП во вкладке «Управление» из списка выберите дверь. В контекстном меню выберите пункт «Настройки». Откроется окно «Настройки двери» (Рисунок 3.77).

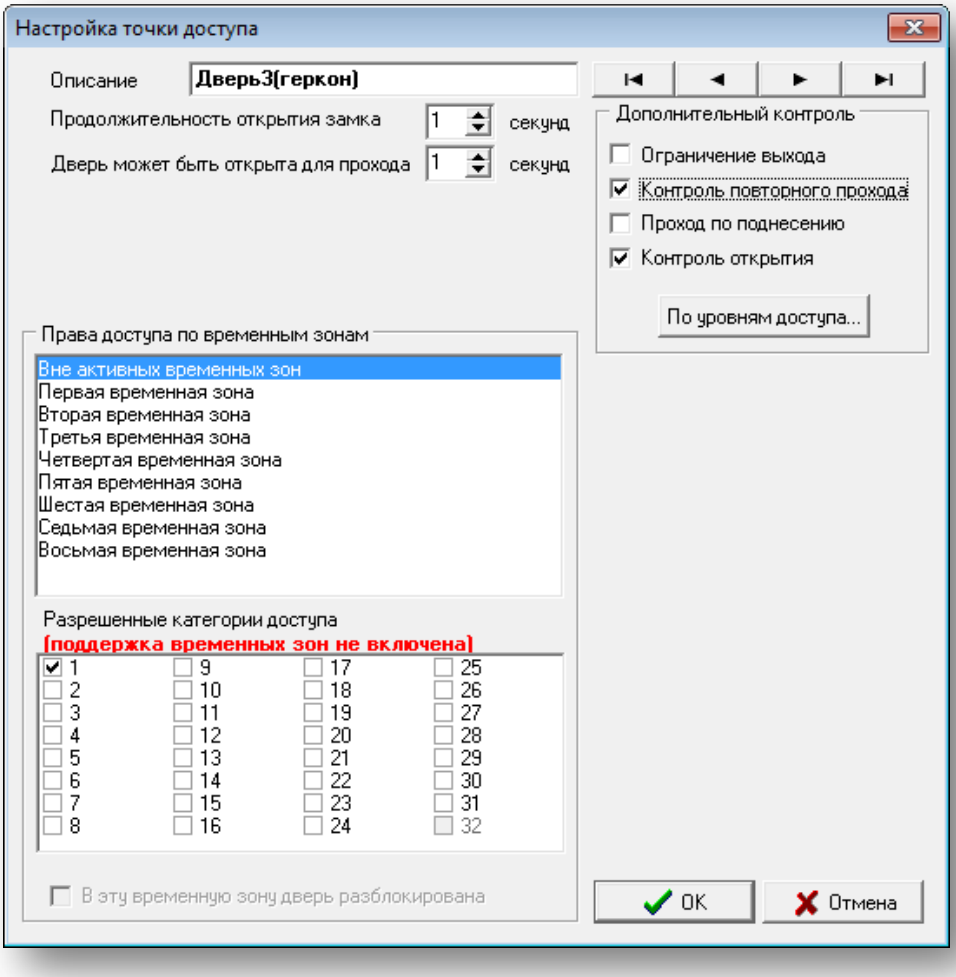


Рисунок 3.77

ПРИМЕЧАНИЕ – Также, окно «Настройки двери» можно вызвать, выбрав пункт «Настройки» в контекстном меню ярлыка двери на вкладке «Планы».

В поле «Дополнительный контроль» необходимо установить флажок «Контроль повторного прохода» и, нажав кнопку «По уровням доступа», в появившемся окне отметить флагом «повторный проход», выбрать уровни доступа (Рисунок 3.78), для которых будет действовать ЗПП. Для сохранения настроек нажмите кнопку «ОК».

SEC.RU | Короткий путь к информации
Скачано с sec.ru

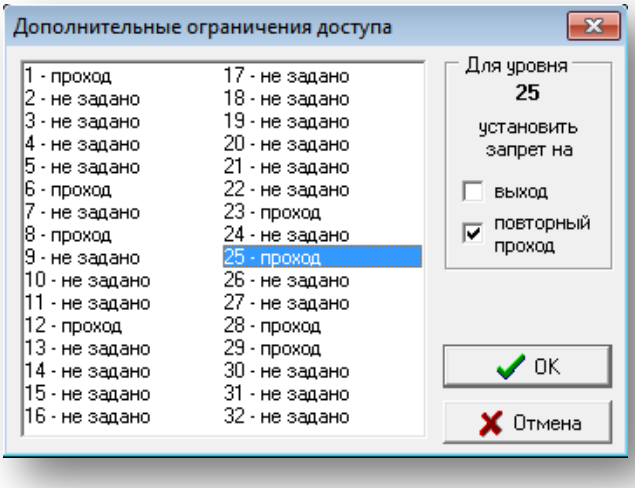


Рисунок 3.78

ПРИМЕЧАНИЕ – В случае потери связи с контроллером доступа при работе глобального ЗПП эта дверь автоматически перейдет в режим локального ЗПП.

3.19 Настройка режима контроля оператора

Режим контроля оператора предназначен для периодического автоматического контроля присутствия оператора на рабочем месте.

Для настройки контроля оператора во вкладке «Управление» нажать кнопку 

.

- В открывшемся окне «Настройка функции контроля оператора» (Рисунок 3.79) снимите флажок «Выключить контроль наличия оператора».

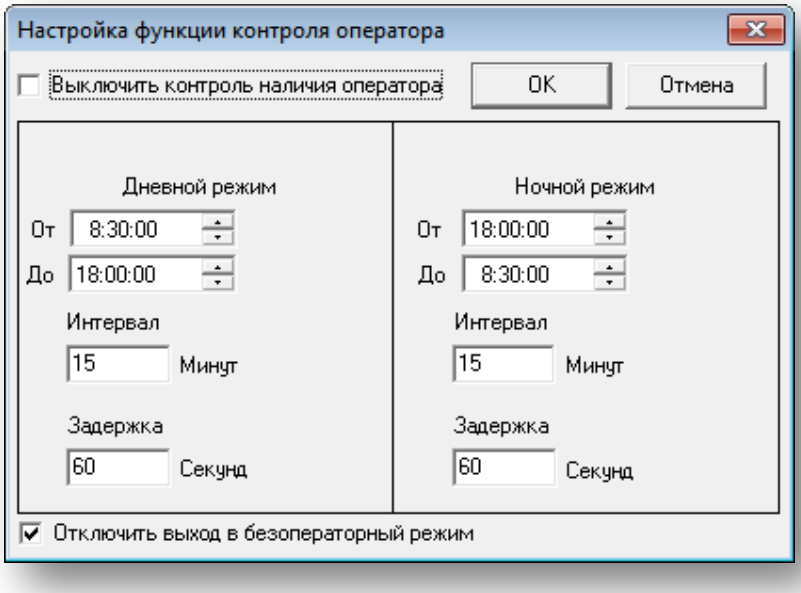


Рисунок 3.79

- Затем в соответствующих полях ввода установите интервал и задержку функции контроля оператора.
- Установите период для дневного и ночного режимов контроля. Если диапазоны дневного и ночного режимов пересекаются, то будут действовать установки параметров, которые имеют наименьшие значения.

SEC.RU | Короткий путь к информации Скачано с sec.ru

По умолчанию программа настроена так, что через заданный промежуток времени (по умолчанию 10 минут), при отсутствии каких-либо действий со стороны оператора, она переходит в безоператорный режим.

- Для отключения выхода в безоператорный режим необходимо поставить флажок «Отключить выход в безоператорный режим».

При включении режима контроля оператора на мониторе через определенные промежутки времени появляется окно (Рисунок 3.80). При корректном выполнении оператором заданного, окно будет закрыто.

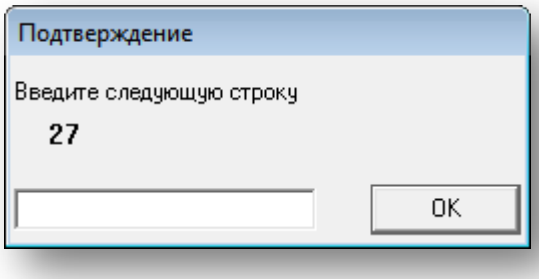


Рисунок 3.80

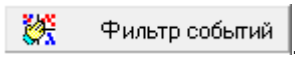
Если оператор проигнорирует запрос, в архиве будет зафиксировано событие «Обнаружено отсутствие оператора».

В случае ошибки при вводе, в архиве событий появится сообщение «Подтверждение оператора с ошибкой».

При выборке данных из архива за определенный период по этим событиям можно будет сделать вывод о дисциплинированности и внимательности операторов.

3.20 Настройка фильтра отображаемых событий

В программе имеется возможность скрывать определенные события вкладки «События в системе».

Для настройки вывода событий во вкладке «Управление» нажмите кнопку 

. В появившемся окне «Настройка фильтра событий» в полях «События в системе» (используя кнопки Shift или Ctrl) либо «События по группам» (отмечая флажками) выбрать события, в отображении которых нет необходимости (Рисунок 3.81).

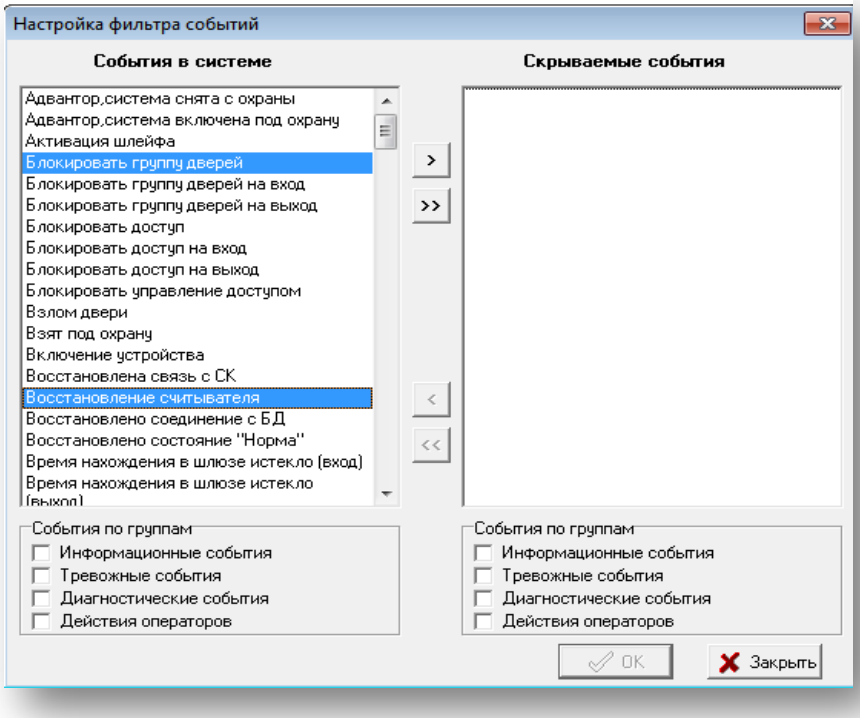


Рисунок 3.81

SEC.RU | Короткий путь к информации
Скачано с sec.ru

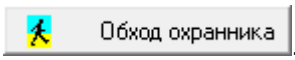
Затем нажать и перенести их в «Скрываемые события». Нажать «ОК» — «Скрываемые события» не будут выводиться во вкладке «События в системе».

Для возврата событий в список отображаемых, следует выделить «Скрываемые события» и нажать . События будут перенесены обратно в список «События в системе».

3.21 Настройка функции контроля обхода охранника

Для объектов, на которых системой безопасности предусмотрен регулярный обход охраняемой территории, в ИКБ «КОДОС» предусмотрена функция контроля охранника.

При совершении обхода охраняемой территории по заданному маршруту, в указанное время охранник подносит кодоноситель к считывателю и в списке событий системы появляется сообщение: «Обход охранника ЧЧ:ММ», с указанием места и времени отметки. В случае опоздания охранника к месту отметки появится сообщение: «Охранник опоздал» с определением места и указанием времени отметки. Если опоздание превысило допустимый интервал, формируется сообщение «Неявка охранника».

Для настройки функции «Обход охранника» во вкладке «Управление» нажмите кнопку 

.

- Для того чтобы назначить новый маршрут, в окне «Настройка обходов охранника» (Рисунок 3.82) в разделе «Маршруты» нажмите кнопку  «Добавить маршрут» — откроется окно «Настройка свойств маршрута» (Рисунок 3.83), далее в строке «Маршрут» введите название маршрута.

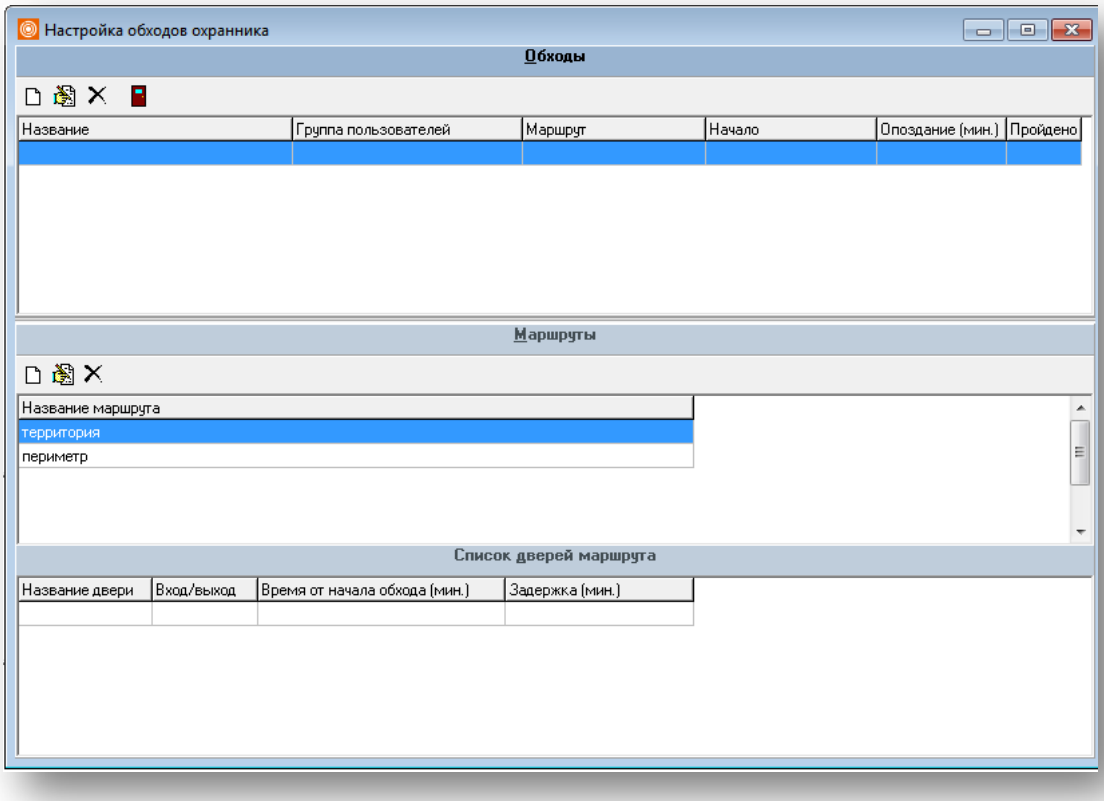


Рисунок 3.82

SEC.RU | Короткий путь к информации
Скачано с sec.ru

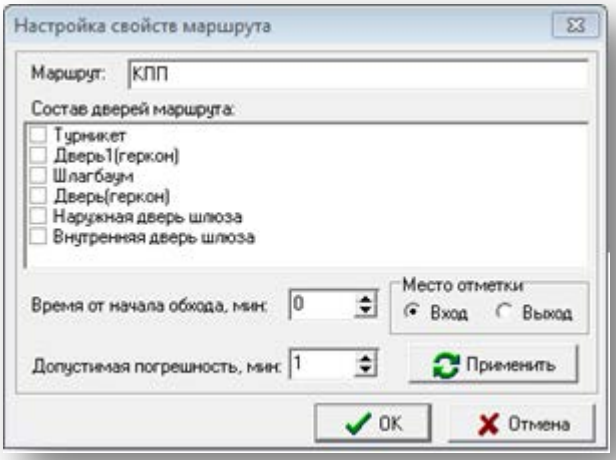


Рисунок 3.83

- Для того чтобы скорректировать уже существующий маршрут или изменить его название, его следует выделить курсором в окне «Настройка обходов охранника» (Рисунок 3.82) в разделе «Маршруты» и нажать кнопку  «Изменить маршрут».
- В окне «Настройка свойств маршрута» (Рисунок 3.84) при необходимости задайте ему новое имя и отметьте флагом точки контроля охранника на маршруте обхода. Каждой выбранной контрольной точке, кроме первой, установите:

«Допустимая погрешность, мин: » — промежуток времени, в течение которого охранник должен пройти через заданную точку прохода и отметиться;

«Время от начала обхода, мин: » — время, устанавливаемое от начала обхода, по прошествии которого охранник должен пройти через заданную точку прохода и отметиться. Далее нажмите кнопку «Применить», а затем перейдите к следующей контрольной точке.

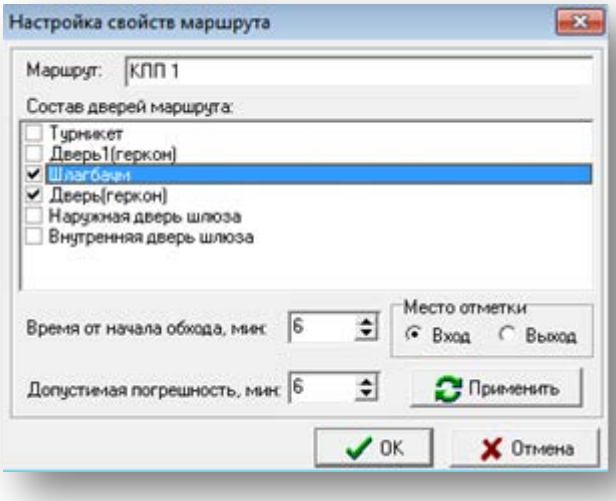


Рисунок 3.84

ВНИМАНИЕ! В один маршрут нельзя дважды включить одну и ту же контрольную точку. В качестве контрольной точки может использоваться считыватель любой двери, в том числе и помещения, в которое охранник не имеет доступа. При выборе контрольных точек необходимо быть внимательным во избежание недоразумений и ложных тревог.

- Для назначения нового обхода нажмите в разделе «Обходы» кнопку «Добавить обход» .
- Для внесения изменений в окне «Настройка обходов охранника» (Рисунок 3.82) следует выделить подлежащий корректировке обход и нажать кнопку  «Изменить обход». В окне «Настройка свойств обхода охранника» (Рисунок 3.85):

SEC.RU | Короткий путь к информации Скачано с sec.ru

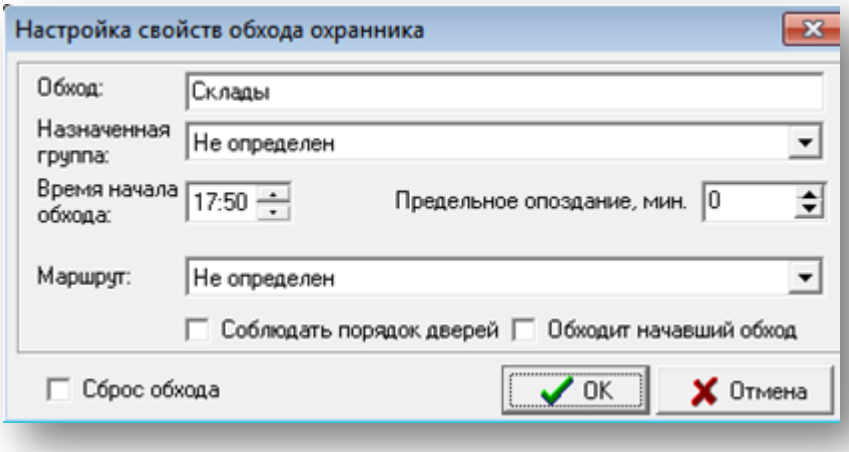


Рисунок 3.85

- В строке «Обход» введите номер или название очередного обхода.
- В поле «Назначенная группа» выберите группу пользователей, из состава которой назначается лицо, совершающее обход.
- В поле «Время начала обхода» установите время начала обхода по одному из заранее заданных маршрутов. Выбор маршрут выбирается в поле «Маршрут». Принимая во внимание, что маршруты устанавливаются с учетом ряда ограничений, в один обход включается только один маршрут.
- Укажите предельно допустимое время опоздания охранника.

ВНИМАНИЕ! Во избежание конфликта данных и возникновения ложной тревоги следует внимательно отнестись к назначению времени начала обхода.

- Условия обхода задайте флажками «Соблюдать порядок дверей» и «Обходит начавший обход». В первом поле устанавливается порядок обхода контрольных точек. Во втором — определяется допустимость выполнения запланированных обходов разными охранниками.
- Установите флаг в поле «Сброс обхода», если по текущему обходу уже были получены некоторые события, но возникла необходимость внести изменения либо в маршрут текущего обхода, либо назначить ему иные условия.

3.22 Настройка свойств двери

Перед началом эксплуатации системы контроля доступом необходимо настроить все точки доступа (двери, турникеты, шлагбаумы и т. д.). Для этого необходимо открыть окно «Настройки двери» (Рисунок 3.86): во вкладке «Управление» нажать кнопку «Настройки» или во вкладке «Планы» одинарным щелчком правой кнопки мыши по ярлыку двери вызвать контекстное меню — далее «Настройки». Выбрать нужную дверь из списка и установить следующие значения:

- «Продолжительность открытия замка» — время, в течение которого замок остается открытым. Если в течение этого времени происходит срабатывание датчика контроля прохода, то замок блокируется. Изменяется в диапазоне от 1 до 30 секунд.
- Параметр «Дверь может быть открыта для прохода» — интервал времени, в который после поднесения к считывателю разрешенной карты и срабатывания датчика прохода система формирует событие «Вход с ключом». Если после поднесения разрешенной карты датчик прохода сработал по истечении заданного интервала времени, система формирует событие «Дверь оставлена открытой». Параметр «Дверь может быть открыта для прохода» изменяется в диапазоне от 1 до 30 секунд.
- Настройка доступа по временным зонам проводится отдельно для каждой временной зоны указанием тех уровней доступа, которым разрешен доступ.
- Если в текущее время ни одна временная зона не активна, то применяются настройки «Вне активных временных зон».

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Для разблокировки отдельной двери в конкретный временной интервал применяется параметр «В эту временную зону дверь разблокирована».
- Установив флаг у параметра «Ограничение выхода», можно настроить запрет на выход определенных категорий пользователей (Рисунок 3.78). Для этого нажмите кнопку «По уровням доступа» в окне «Настройки двери».
- Параметр «Контроль повторного прохода» включает режим локального ЗПП для указанных групп доступа.
- При установке флага «Проход по поднесению» факт прохода пользователя будет засчитываться при поднесении разрешенной карты к считывателю. При этом дополнительное действие по открытию двери (срабатыванию датчика прохода) необязательно. Данный режим используется при оборудовании мест учета рабочего времени без монтажа оборудования СКУД (дверей, замков, герконов).

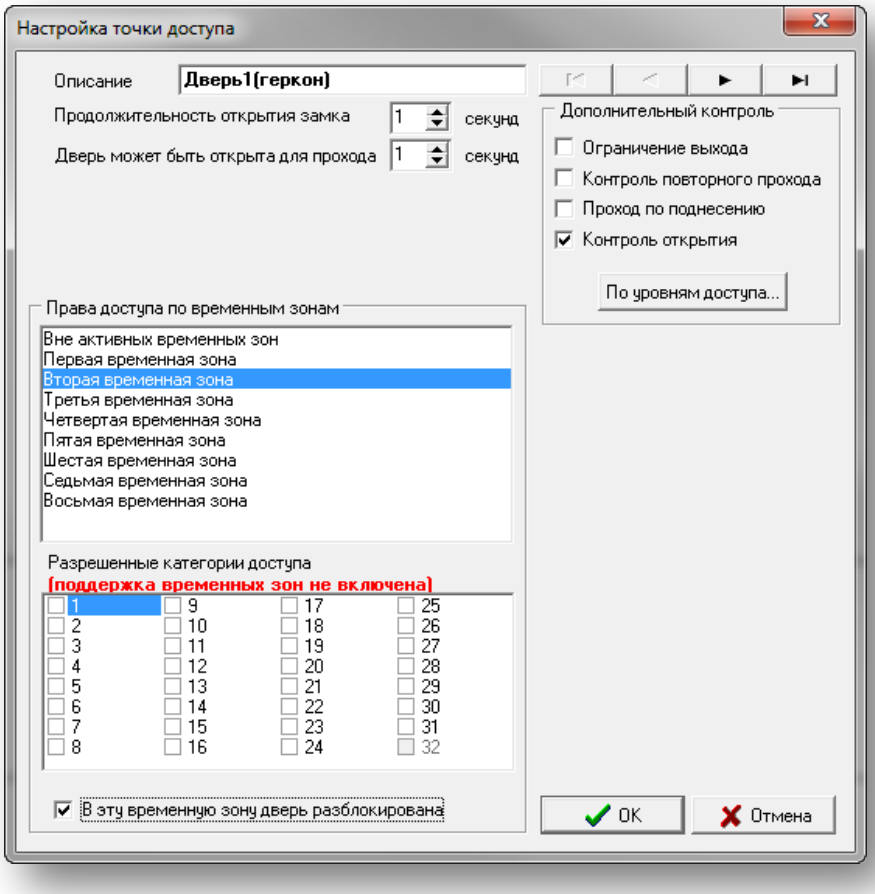


Рисунок 3.86

3.23 Настройка «Кабинетного режима»

Для контроллеров доступа серии «КОДОС ЕС-ХХХ М» реализована функция кабинетного режима.

Кабинетный режим — это совокупность режимов работы контроллера: «Свободный проход», «Охрана», «Свободный доступ», «Ограничение доступа», представляющих собой заранее разработанные сценарии поведения системы.

- «Свободный проход» — режим позволяет беспрепятственно осуществлять проход в точку доступа при наличии привилегированной карты, вне зависимости от других ограничений системы, кроме установленных на данной точке прохода режимах «Ограничение доступа» и «Охрана».
- «Охрана» — в этом режиме дверь заблокирована и закрыта для прохода, контролируется состояние датчиков. Постановка и снятие этого режим возможны с помощью кодоносителя с правом постановки на охрану или командой с ПК.
- Режим «Свободный доступ» обеспечивает долговременную разблокировку замка для обеспечения беспрепятственного прохода. Управление режимом выполняется с помощью привилегированной карты доступа или или командой с ПК.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- Режим «Ограничение доступа» запрещает проход для всех категорий пользователей. После отмены режима, доступ в точку прохода восстанавливается в соответствии с настройками системы.

Переведение контроллера в любой из этих режимов означает настройку определенного сценария работы системы, которая может выполняться из программы либо с помощью карты доступа.

3.23.1 Изменение режима работы контроллера с помощью ПО ИКБ «КОДОС»

- Во вкладке «Планы» выберите точку доступа, контролируемую контроллером серии «КОДОС ЕС-XXX М». В ее контекстном меню выберите пункт, определяющий режим работы контроллера.
- Также, во вкладке «Доступ» в таблице «Группы дверей/ Двери» выберите точку доступа, контролируемую контроллером серии «КОДОС ЕС-XXX М». В панели инструментов вкладки нажмите кнопку, отвечающую за определенный режим работы контроллера. Подробнее о настройках см. «Руководство оператора ИКБ „КОДОС“».

3.23.2 Управление режимами контроллеров серии «КОДОС ЕС-XXX М» с помощью карты доступа.

Контроллеры «КОДОС ЕС-202 М» и «КОДОС ЕС-304 М» поддерживают функцию кабинетного режима. Для этих контроллеров можно назначить до восьми привилегированных карт. Привилегированные карты — это карты, с помощью которых владелец может назначать контроллеру любой из описанных выше режимов работы.

Привилегированные карты добавляются из числа уже существующих в базе данных.

Настройка

- Во вкладке «Управление» выберите точку доступа, управляемую контроллером, поддерживающим кабинетный режим, и нажмите кнопку «Настройки».
- В разделе «Управление по карте» отметьте флагами режимы, которые сможет устанавливать владелец привилегированной карты.
- В окне «Настройка точки доступа» (Рисунок 3.87) нажмите кнопку «Права».

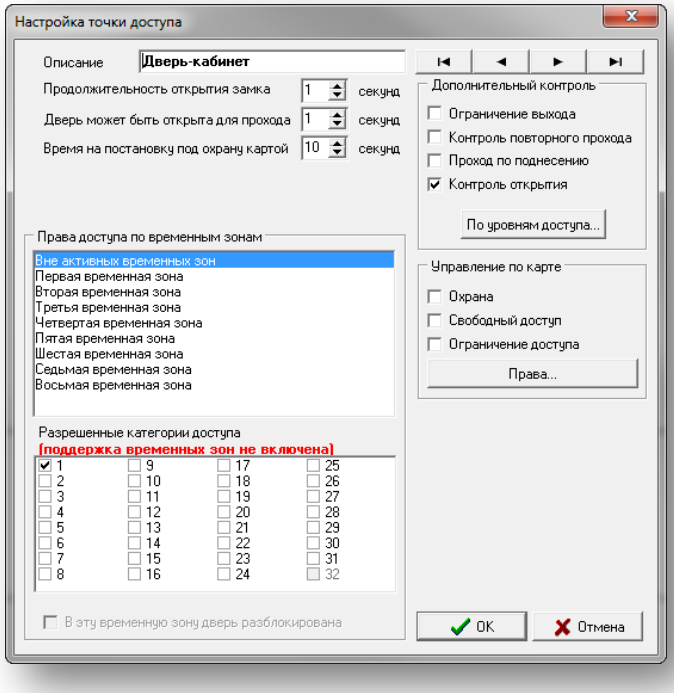


Рисунок 3.87

Откроется окно «Привилегированные карты и права на управление» (Рисунок 3.88).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

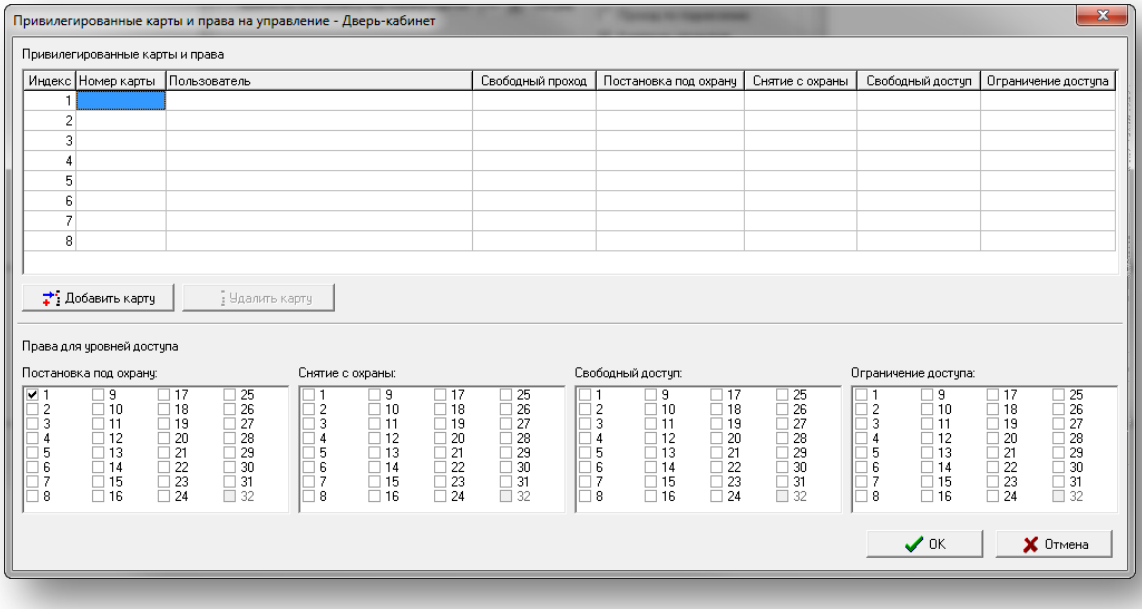


Рисунок 3.88

Раздел «Права для уровней доступа»

В каждом из разделов: «Постановка на охрану», «Снятие с охраны», «Свободный доступ», «Ограничение доступа» укажите уровни доступа (не привилегированных) карт пользователей, которым будет разрешено, соответственно, ставить помещение на охрану, снимать с охраны, устанавливать контроллеру режим «Свободный доступ», а также управлять режимом «Ограничение доступа».

Раздел «Привилегированные карты и права»

- «Индекс» — значение, присваиваемое карте из списка привилегированных, в отдельном разделе памяти контроллера.
- «Номер карты» — номер учетной записи пользователя, берется из списка во вкладке «Пользователи».
- «Пользователь» — имя пользователя в системе.
- «Свободный проход» — установленный флаг в этом поле дает пользователю право прохода в эту точку доступа, даже если ранее доступа в эту дверь у него не было. Кроме того, разрешение на проход в эту точку доступа прописывается также и во вкладке «Пользователи». В окне «Редактирование карточки пользователя» → вкладке «Доступ» (Рисунок 3.89) запись будет выделена красным цветом; установленный напротив нее флажок снять нельзя.
- «Постановка на охрану» — владелец привилегированной карты может ставить на охрану подключённые к этому контроллеру датчики/ двери.
- «Снятие с охраны» — владелец привилегированной карты может снимать с охраны подключённые к этому контроллеру датчики/ двери.
- «Свободный доступ» — установленный флаг в этом поле дает право владельцу привилегированной карты переводить контроллер в состояние «Открыто».
- «Ограничение доступа» — право позволяет владельцу привилегированной карты переводить контроллер в состояние «Блокировано».

SEC.RU | Короткий путь к информации
Скачано с sec.ru

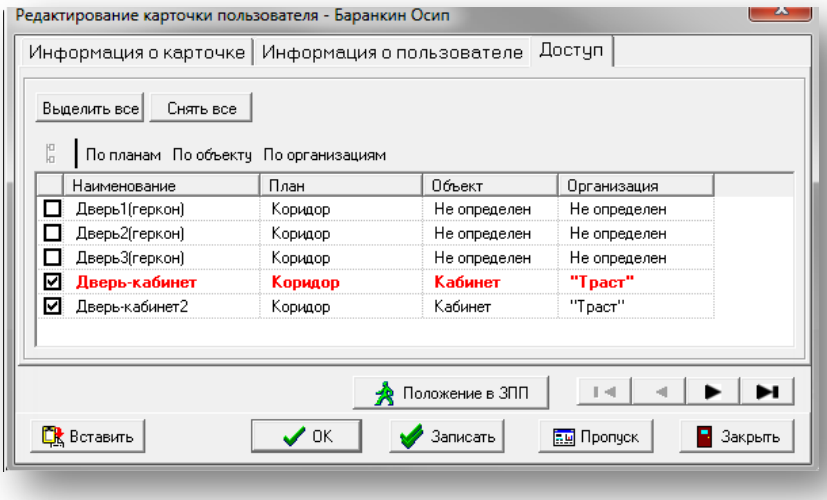


Рисунок 3.89

ПРИМЕЧАНИЕ – Владелец не привилегированной карты может изменять режим работы контроллеров «КОДОС ЕС-202 М» и «КОДОС ЕС-304 М» при следующих условиях:
- кодоносителям с этим уровнем доступа разрешено устанавливать определенный режим работы контроллера (Рисунок 3.91);
- при редактировании учетной записи пользователю разрешен проход в эту точку доступа (Рисунок 3.89).

- Для добавления привилегированной карты в окне «Привилегированные карты и права на управление» нажмите кнопку «Добавить карту» (Рисунок 3.88).
- В открывшемся окне «Выбор пользователя» (Рисунок 3.90) выберите карту сотрудника и нажмите «ОК».

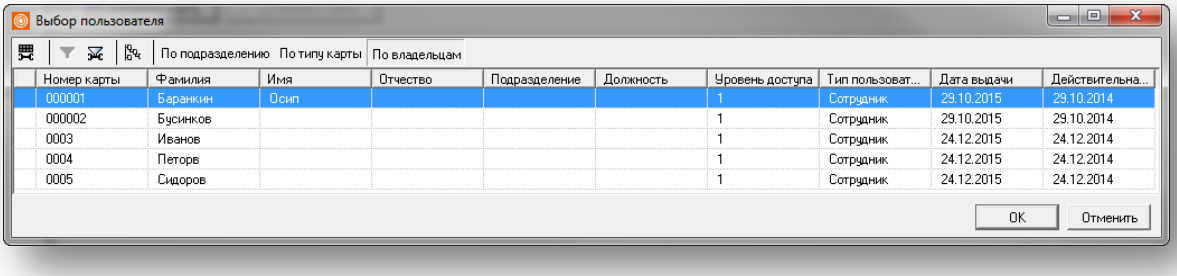


Рисунок 3.90

Запись будет добавлена в таблицу окна «Привилегированные карты и права на управление»(Рисунок 3.91).

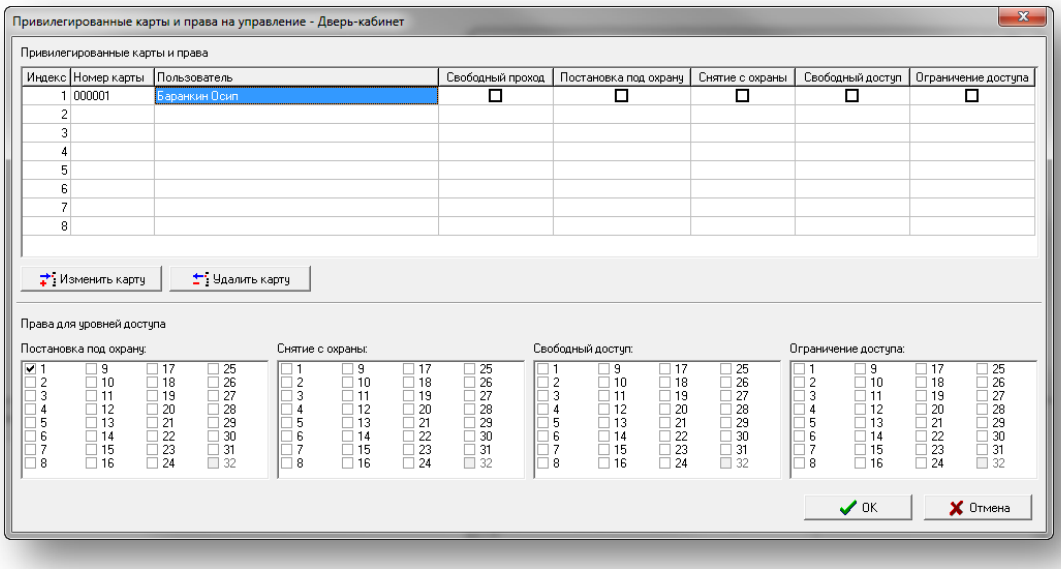


Рисунок 3.91

SEC.RU | Короткий путь к информации
Скачано с sec.ru

При необходимости можно заменить одну из выбранных привилегированных карт доступа другой. Для этого выберите из списка привилегированную карту, подлежащую замене, затем нажмите кнопку «Изменить карту» и укажите карту другого пользователя (Рисунок 3.91).

Для удаления привилегированной карты из списка нажмите кнопку «Удалить карту». В завершение настроек нажмите «ОК». Для отмены внесенных изменений нажмите кнопку «Отмена».

Сортировка и фильтры

Существует возможность сортировать строки таблицы (Рисунок 3.90) по заголовку столбца.

Для удобства просмотра элементов списка можно сгруппировать их по подразделению, типу карты или по владельцам. При выборе любого из перечисленных условий станет активной кнопка , предназначенная для сворачивания или разворачивания представленных в списке групп. При нажатии кнопки в списке будут представлены пользователи системы, упорядоченные в соответствии с выбранным типом сортировки.

Кроме того, можно настроить параметры отображения столбцов таблицы пользователей. Для этого в панели инструментов окна «Выбор пользователей» нажмите кнопку «Настройка столбцов». В окне «Настройка столбцов» (Рисунок 3.92), снимая или устанавливая флаги напротив названия столбца, можно включать или исключать его из таблицы. Также, при помощи стрелок . можно изменять расположение столбца в таблице (влево – вправо). Для этого нужно выделить мышью название столбца, а затем стрелками переместить строку. Далее нажмите кнопку «Применить».

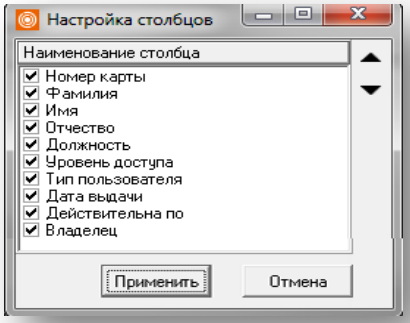


Рисунок 3.92

Если таблица со списком пользователей системы (Рисунок 3.90) значительная по объёму, для удобства работы с ней рекомендуется настроить условия отбора элементов таблицы.

- В панели инструментов окна «Выбор пользователей» нажмите кнопку «Настройки фильтра».
- В открывшемся окне «Настройки фильтра» (Рисунок 3.93) нажмите кнопку , чтобы добавить новое условие отбора данных.
- В окне «Условие» выберите из выпадающих списков параметр, условие (равно или не равно) и присвойте значение.
- Нажмите «Добавить», «ОК», а затем кнопку включения/ выключения фильтра . Состав строк в списке окна «Выбор пользователя» (Рисунок 3.90) будет изменен в соответствии с заданным критерием.
- Если в качестве условия выбрать «Не равно», для отображения в списке будут выбраны элементы, параметры которых не будут соответствовать введенному значению.
- Для редактирования условий отбора элементов в окне «Настройки фильтра» (Рисунок 3.93) выделите строку с условием, которое нужно изменить, нажмите кнопку и внесите необходимые коррективы. Затем нажмите кнопку «Изменить» и «ОК».
- Нажатие кнопки удаляет выделенное условие.
- Стрелки перемещают запись с условием вверх или вниз.
- Кнопка Очистить фильтр удаляет все условия.

SEC.RU | Короткий путь к информации Скачано с sec.ru

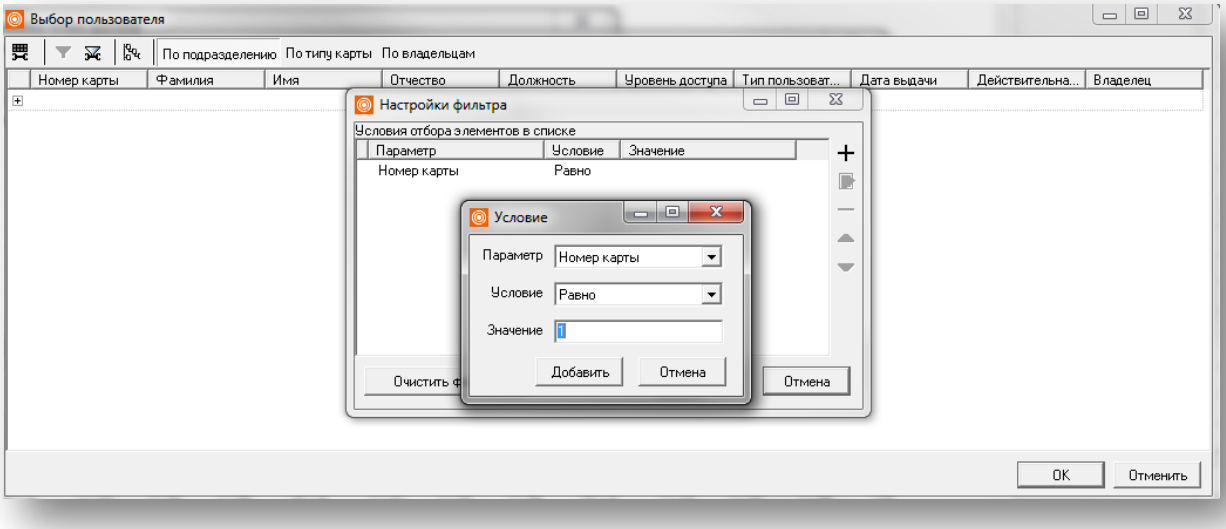


Рисунок 3.93

3.24 Настройка исполнительного устройства для «КОДОС ЕС-202 М» и «КОДОС ЕС-304 М»

В ИКБ реализована возможность устанавливать настройки привязанным к контроллерам «КОДОС ЕС-202 М» и «КОДОС ЕС-304 М» исполнительным устройствам.

- Для этого во вкладке «Управление» выберите искомое устройство (Рисунок 3.94).
-

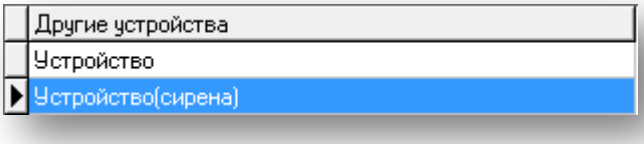


Рисунок 3.94

- Кнопка «Настройка устройства» станет активной.
- По нажатию этой кнопки откроется окно для внесения настроек выбранному исполнительному устройству.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

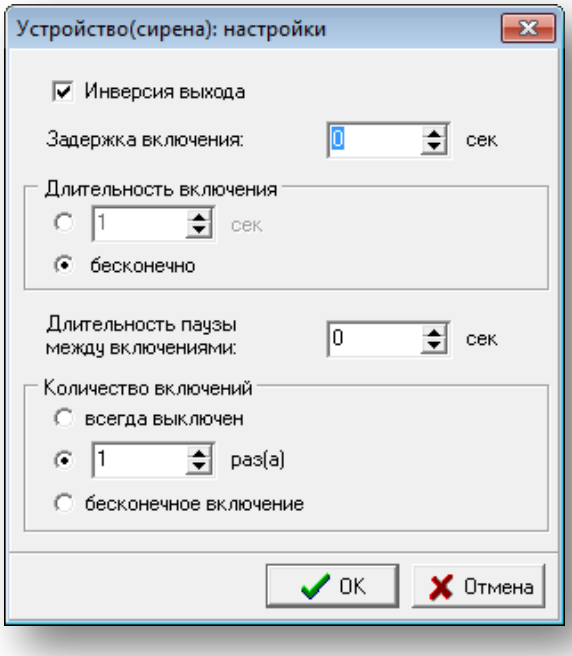


Рисунок 3.95

- «Инверсия выхода» — установите флаг, если в дежурном состоянии устройство пропускает ток.
- «Задержка включения» — установите в поле с пошаговым изменением значения время задержки перед включением устройства.
- «Длительность включения» — укажите время, на протяжении которого устройство будет работать.
- «Длительность паузы между включениями» — в поле с пошаговым изменением значения установите временной интервал между включениями устройства.
- В разделе «Количество включений» выберите режим работы устройства по срабатыванию датчика: всегда выключено; бесконечное включение; или задайте требуемое количество включений.

3.25 Особенности настройки контроллера шлюза

Контроллер шлюза настраивается аналогично контроллеру двери. Кроме того, в окне «Настройка двери» становится активным параметр «Время нахождения в шлюзе» (Рисунок 3.96).

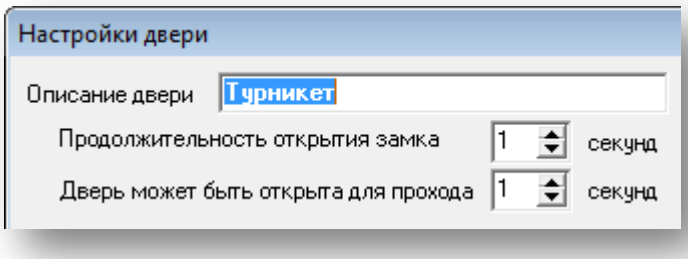


Рисунок 3.96

Параметр «Время нахождения в шлюзе» устанавливает максимальное время, в течение которого должен быть завершен проход через шлюз. В это время блокируются считыватели дверей, и вход в шлюз с обеих сторон запрещен. Логика работы данной конфигурации реализована на аппаратном уровне и заключается в следующем: при прохождении на охраняемый объект владелец электронной карты, идентифицировав себя поднесением ее ко входному считывателю, заходит внутрь шлюза и закрывает за собой дверь. В этот момент работа считывателей обеих дверей на определенное время (время нахождения в шлюзе) блокируется контроллером. В этот момент считывание карты другого пользователя (как со стороны входа, так и со стороны выхода) и, соответственно, его проход в шлюз невозможны.

После того как владелец электронной карты зашел в шлюз, обязательным условием дальнейшего прохода является закрытие за собой входной двери. До тех пор, пока входная дверь остается открытой, кнопка

SEC.RU | Короткий путь к информации Скачано с sec.ru

REX выходной двери заблокирована — проход на объект невозможен. Считыватель с внешней стороны выходной двери в этот момент также заблокирован.

После выполнения вошедшим (либо сотрудником службы безопасности) процедур, предусмотренных режимом охраны объекта, сотрудник службы безопасности, в зависимости от принятого решения, нажимает одну из кнопок открытия двери (REX):

- либо кнопку открытия второй двери для дальнейшего прохода владельца электронной карты;
- либо кнопку первой двери — для того, чтобы вошедший покинул шлюз, не заходя на охраняемый объект.

После прохода владельца карты через шлюз и закрытия выходной двери (либо входной двери при запрещении доступа на объект и выходе в обратном направлении) блокировка считывателей снимается и становится возможной идентификация кода электронной карты следующего проходящего через шлюз.

При выходе владельца электронной карты с охраняемого объекта алгоритм прохода через шлюз соответствует описанию выше.

Также, возможна и программная реализация шлюза. Данная конфигурация строится на контроллерах доступа (EC-202, EC-502) и основана на установке правил (см. Настройка правил).

Для этого необходимо:

1. создать группу дверей (туда должны войти 2 или более дверей шлюза);
2. создать два правила для этой группы:
    - «открыта дверь группы (тамбура)» — «заблокировать группу дверей на вход и выход»;
    - «закрыты все двери группы» — «разрешить группе дверей открываться на вход и на выход».

Алгоритм работы можно понять из содержания этих правил: когда одна дверь в шлюзе открыта, то остальные обычным образом открыть нельзя — они будут разблокированы только после закрытия этой двери.

ПРИМЕЧАНИЕ – Для программной реализации работы шлюза прошивка контроллеров должна быть версии 1.6 и более новой. Так как данная логика работы реализована на программном уровне, то она будет работать только в он-лайн режиме (при запущенной программе «Сервер ИКБ» и наличии связи с ним).

3.26 Настройка картоприемника

Откройте окно свойств турникета и установите, если необходимо, категории доступа и параметры «Ограничение выхода» и «Контроль повторного прохода» (Рисунок 3.97).

SEC.RU | Короткий путь к информации Скачано с sec.ru

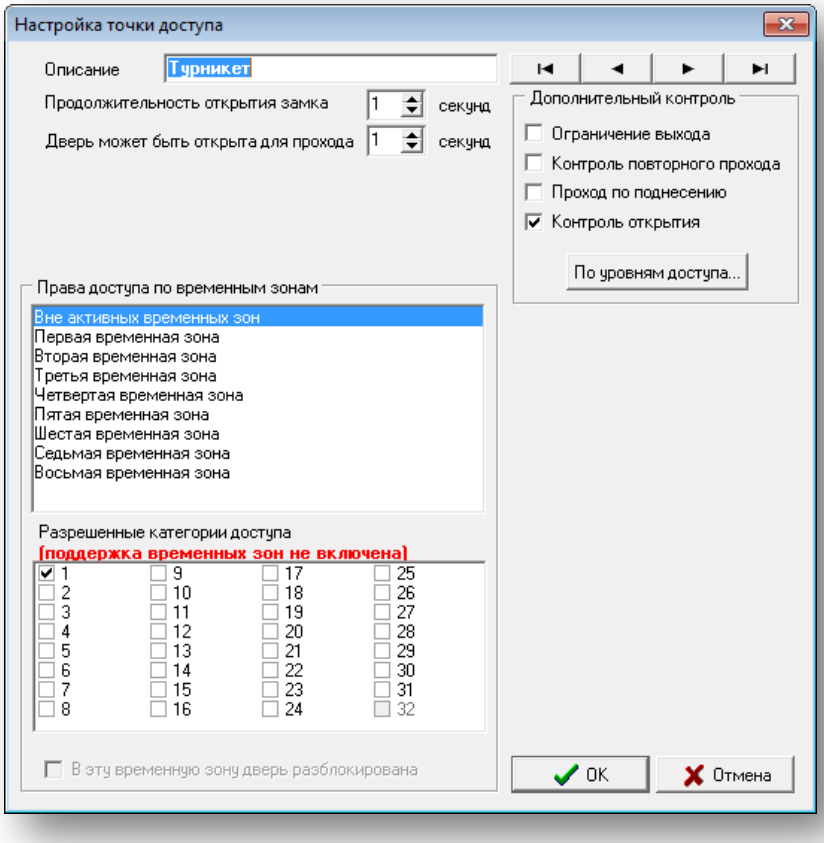


Рисунок 3.97

ПРИМЕЧАНИЕ – Уровни доступа у карт сотрудников и гостевых карт должны быть различны. Уровень доступа для гостевых карт должен совпадать с группой доступа, установленной в программе «Бюро пропусков» (по умолчанию — 25).

Нажмите кнопку «По уровням доступа». В открывшемся окне установите запрет на выход для гостевых карт (Рисунок 3.98).

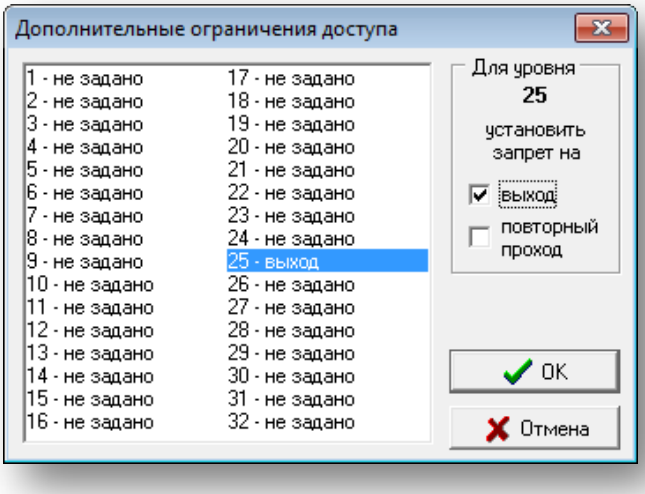
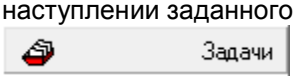


Рисунок 3.98

- Запрет на повторный проход для гостевых карт устанавливать нельзя. Выход для гостевых карт через данную точку прохода осуществляется через отдельный контроллер (контроллер картоприемника). Поэтому для контроллера доступа всегда проход осуществляется в одном направлении.
- При работе контроллера в автономном режиме выходы через картоприемник не отрабатываются.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.27 Планировщик задач

В ИКБ «КОДОС» существует возможность программировать выполнение определенных действий при наступлении заданного момента времени. Для настройки планировщика задач нажмите кнопку 

во вкладке «Управление». Для создания новой задачи нажмите кнопку «Добавить» (Рисунок 3.99).

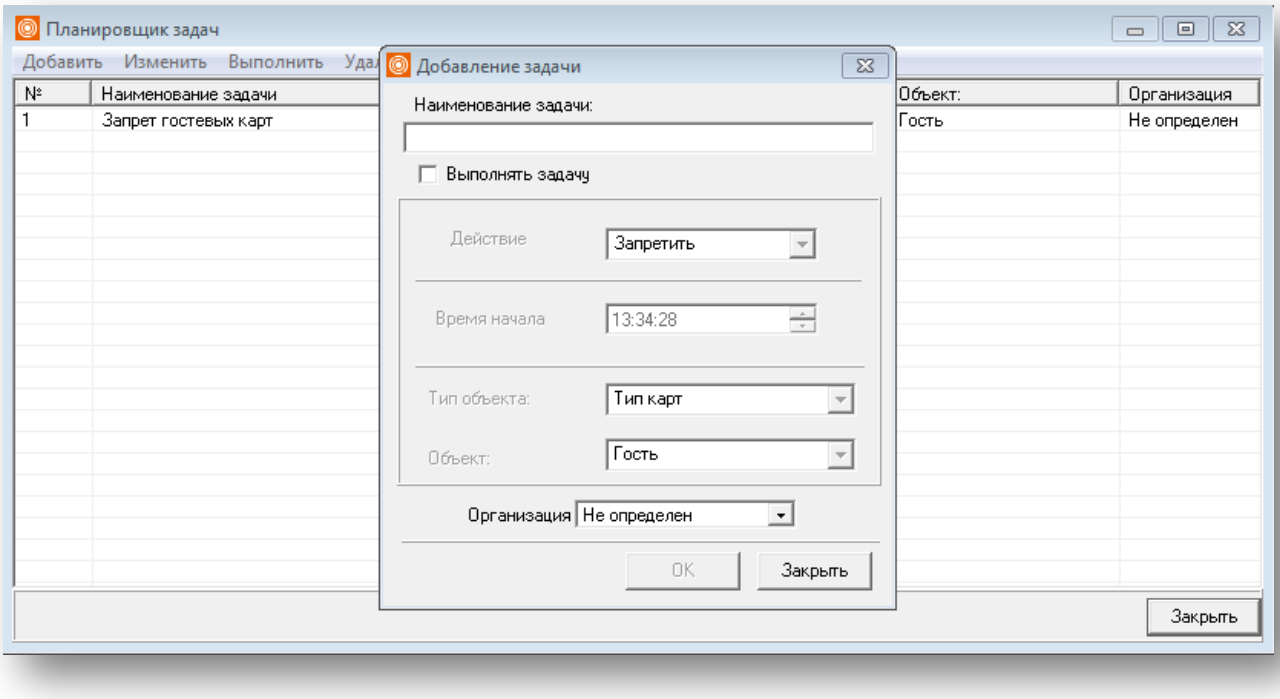


Рисунок 3.99

- В поле «Наименование задачи» окна «Добавление задачи» укажите выполняемое действие. Параметр «Выполнять задачу» определяет, будет ли выполняться задача или нет. Для выполнения любой задачи в текущий момент времени необходимо установить флаг «Выполнять задачу». При снятии галочки задача останется в базе данных, но при наступлении указанного момента времени выполняться не будет.

ПРИМЕЧАНИЕ – В текущей версии программы доступно только одно действие: «Запретить»

Для установки времени выполнения задачи установите его значение в поле «Время начала». Задание будет выполняться ежедневно в указанное время.

- В поле «Тип объекта» доступны следующие значения: «Тип карт», «Группа пользователей», «Карта».
- В поле «Объект» доступны значения, соответствующие выбранному типу объекта.

3.28 Настройка функции отложенного опроса панелей «А-20»

При запуске ИКБ автоматически проводит опрос панелей А-20. В течение этого времени у пользователя нет возможности внести изменения в настройки. Для удобства управления А-20 существует функция отложенного опроса:

- Запустить «Сервер ИКБ». Время, чтобы отложить опрос, по умолчанию составляет 10 минут. Таймер автоматически начнет обратный отсчет, по завершении которого система начнет опрос панелей.
- Если необходимо настроить параметры А-20, нажмите кнопку «Отложить опрос», временные показатели таймера обновятся — у пользователя будет час, чтобы внести необходимые изменения и загрузить настройки в А-20.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4 ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ ПРОГРАММЫ

4.1 Установка и настройка USB-считывателя

При большом количестве карт и значительном расстоянии от считывателя до компьютера с соответствующим ПО, определение номеров карт может быть связано с рядом неудобств и вероятностью ошибки. В этом случае целесообразно использовать считыватель, подключаемый через USB-порт компьютера.

- Подключите USB-считыватель к USB-порту компьютера.
- Запустите «Диспетчер устройств», в контекстном меню USB<-> Serial выберите пункт «Свойства» (Рисунок 4.1).

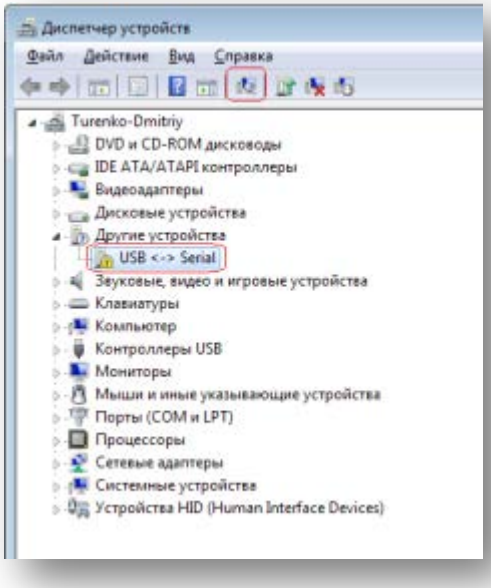


Рисунок 4.1

- В окне «Свойства USB» во вкладке «Драйвер» нажмите «Обновить» и «ОК» (Рисунок 4.2).

SEC.RU | Короткий путь к информации Скачано с sec.ru

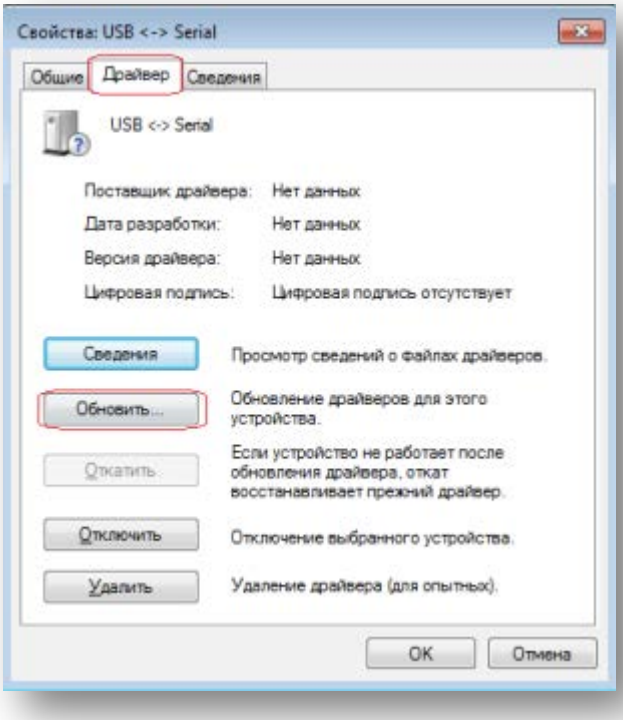


Рисунок 4.2

- В окне «Обновление драйверов» выберите «Выполнить поиск драйверов на этом компьютере» (Рисунок 4.3).

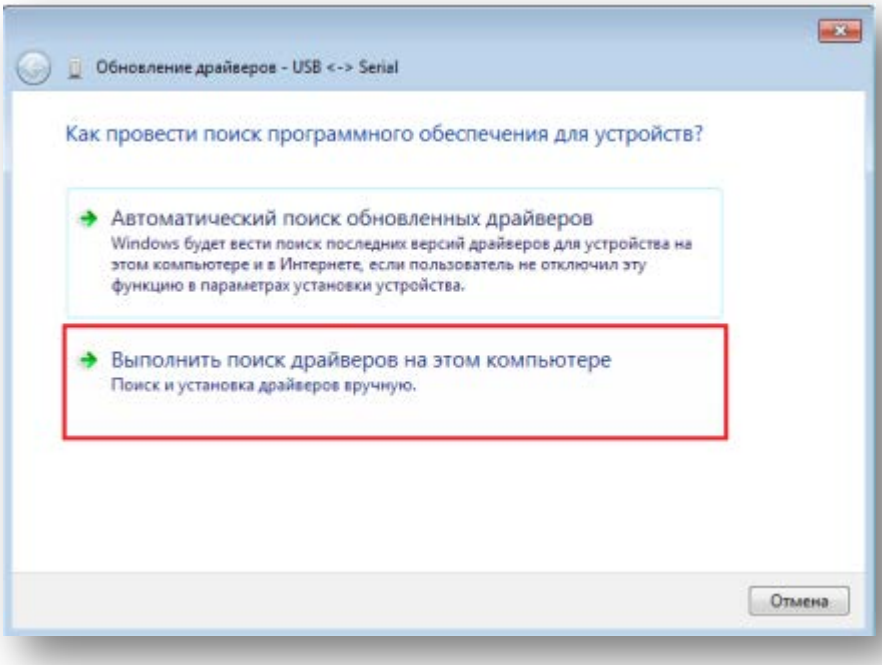


Рисунок 4.3

- Вставьте диск с драйверами в дисковод. В окне выбора места размещения драйверов укажите путь к диску с драйверами «Диск:\ Drv». Нажмите кнопку «Далее» (Рисунок 4.4).

SEC.RU | Короткий путь к информации Скачано с sec.ru

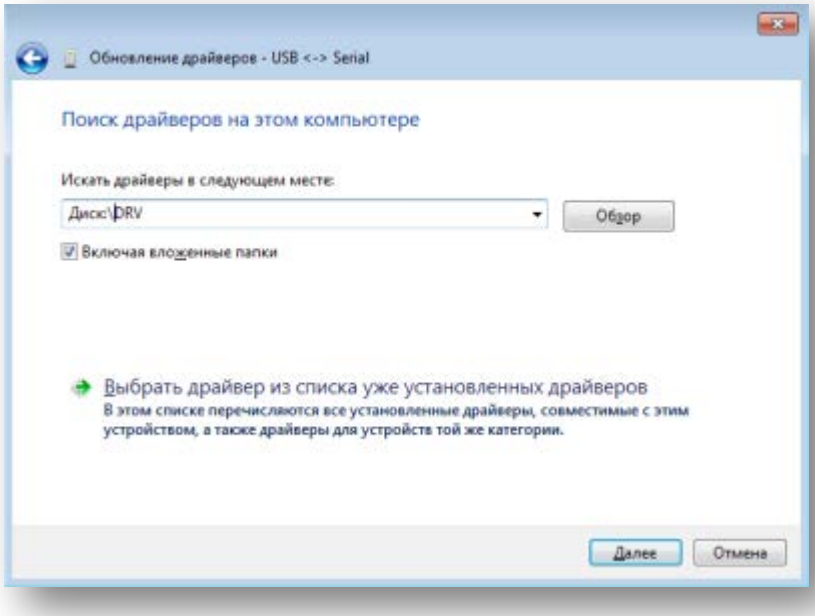


Рисунок 4.4

- После того, как мастер подключения оборудования выдаст сообщение о нахождении драйвера и готовности к установке, нажмите кнопку «Далее», после чего начнется установка программы. По окончании установки драйверов проверьте новое устройство. В контекстном меню: «Компьютер» → «Свойства» → «Оборудование» → «Диспетчер устройств» → «Порты (COM и LPT)» → «USBSerialPort(COM_)». Считыватель, подключенный к USB-порту, идентифицируется как еще один COM-порт с очередным номером (Рисунок 4.5).

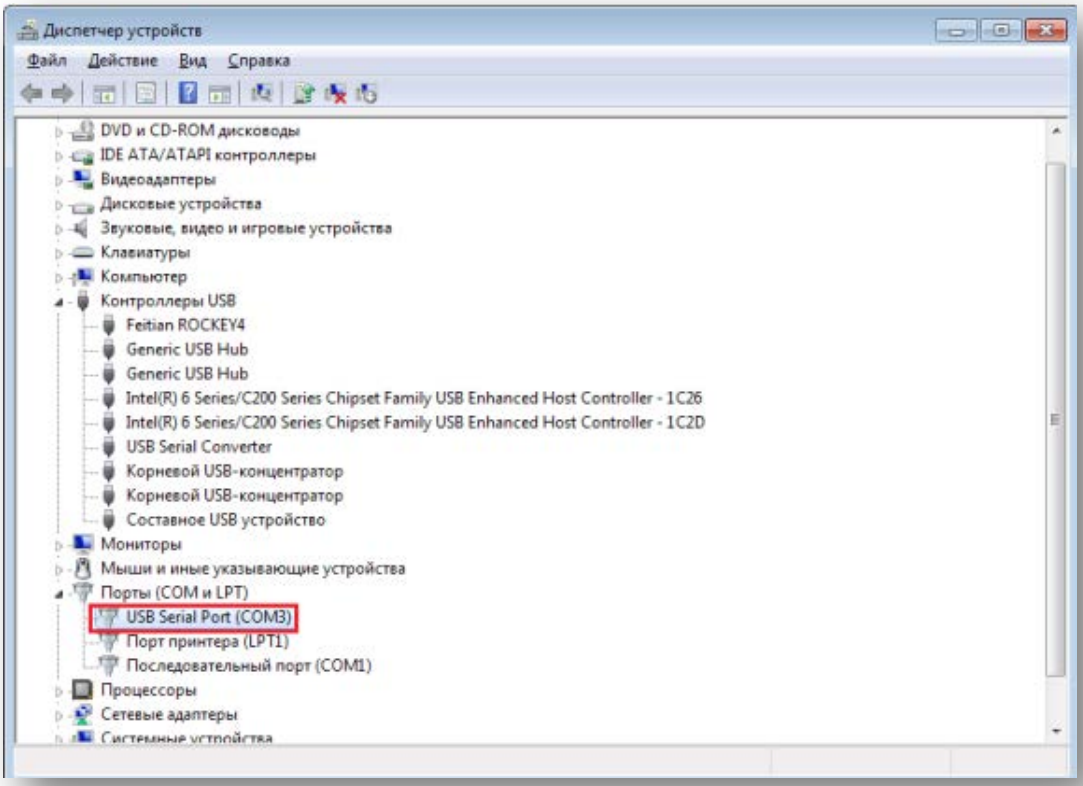


Рисунок 4.5

- Далее необходимо указать значения в полях «Имя последовательного порта» и скорость передачи последовательного порта» (подробнее см. п. Вкладка «Основные параметры».

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- Укажите тот номер COM-порта, который указан в «Диспетчере устройств».
- Перезапустите «Сервер ИКБ», чтобы внесенные изменения вступили в силу.

При подключенном USB-считывателе в статус баре в правой нижней части главного окна программы появится иконка считывателя. Различают три состояния:

- Иконка серого цвета — настройки USB –считывателя прописаны, но само устройство не подключено к USB-порту.
- Иконка красного цвета — считыватель подключен.
- Иконка зеленого цвета — считывается карта.

4.2 Настройка модуля «Персонализации карт»

ПРИМЕЧАНИЕ – Возможность добавления фотографии пользователя определяется наличием лицензии на «Модуль персонализации карт доступа и печати пропусков». При отсутствии лицензии функция будет недоступна. Для добавления модуля обратитесь к представителям ОАО «Бауманн».

Если предполагается создавать фотографии с помощью видеокамеры, чтобы изображение было нужного качества, необходимо заблаговременно подготовить место для фотографирования и настроить видеооборудование.

При использовании сетевой видеокамеры в качестве видеоисточника модуля персонализации необходимо запустить «Конфигуратор». Далее ввести логин и пароль. В контекстном меню к компьютеру (ПК), на котором установлен сервер ИКБ «КОДОС», необходимо добавить ПК-видеосервер, а уже к нему — видеоисточник (Рисунок 4.6).

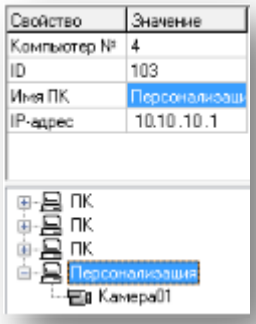


Рисунок 4.6

В окне «Редактирование свойств видеоисточника» установите флаг «Источник модуля персонализации» (Рисунок 4.7).

ПРИМЕЧАНИЕ – Кроме того, необходимо во вкладке «Управление» → кнопка «Настройка АРМ» → в разделе «Камеры» указать системное имя источника видеоизображения (подробнее см. Настройка АРМ).

SEC.RU | Короткий путь к информации Скачано с sec.ru

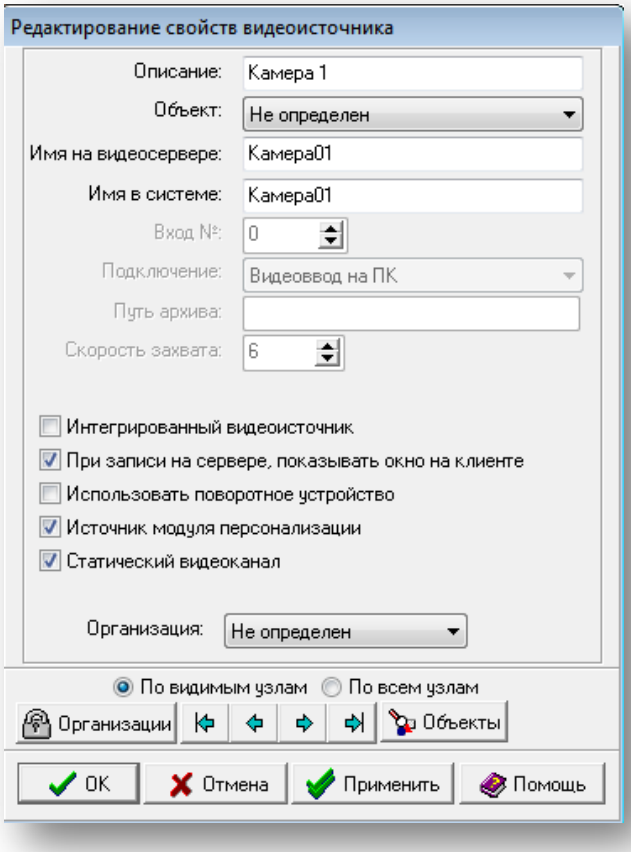


Рисунок 4.7

4.3 Настройка модуля «Учет и выдача карт посетителям»

ПРИМЕЧАНИЕ – Модуль «Учета карт посетителей» доступен только при наличии соответствующей лицензии. Для включения модуля в состав системы обратитесь к представителям ОАО «Бауманн». Процесс проверки и ввода лицензии описан в разделе 2.5«Защита ПО «КОДОС» от несанкционированного использования.

Модуль «Учета карт посетителей» (далее Модуль) предназначен для учета выданных посетителям охраняемого объекта карт доступа — пластиковых кодоносителей, разграничивающих проход на охраняемый объект. К функциям модуля относятся:

- просмотр в базе данных списка посетителей и перечня выданных карт;
- поиск посетителя или карты в списках по заданным критериям;
- изменение статуса карт доступа и т. п.

Модуль может работать как на сервере ИКБ, так и на компьютере с установленной программой «Администратор ИКБ».

Принципы работы

- Объектами учета Модуля являются временные посетители.
- Для входа на охраняемый объект каждому посетителю выдаётся карта доступа — гостевая карта.
- Коды выдаваемых карт, соответствующие им уровни доступа учитываются в базе данных ИКБ (в СКУД).
- Каждый проход посетителя через точки доступа фиксируется в архиве событий Системы.
- Покидая объект, посетитель возвращает карту, которая может быть использована для повторной выдачи с соответствующим изменением учетной записи в базе данных.

С помощью функций Модуля информация о посетителе, например ФИО, фотография или копия документа, удостоверяющего личность, заносится в базу данных учета и выдачи карт, что позволяет сотруднику службы безопасности:

- идентифицировать человека, проходящего через точки доступа;

SEC.RU | Короткий путь к информации Скачано с sec.ru

- вести статистику посещений;
- отследить по архиву событий Системы маршрут и график перемещений каждого из посетителей;
- оперативно менять статус карт доступа.

4.4 Настройка модуля «Дизайн пропусков»

При установке программы пользователю доступно только две схемы пропусков: «Голубая1» и «Голубая2». Однако существует возможность создать и собственную схему.

ПРИМЕЧАНИЕ – Создание собственных схем пропусков возможно только при наличии лицензии на «Модуль дизайна пропусков». Процесс проверки и ввода лицензии описан в п. Защита ПО «КОДОС» от несанкционированного использования. В случае, если Вы планируете включить «Модуль дизайна пропусков» в состав Системы, обратитесь к представителям ОАО «Бауманн».

Установка «Модуля дизайна пропусков возможна как на компьютере с установленными программами «Сервер ИКБ», «Администратор ИКБ», так и на любой другой компьютер. Необходимым условием является наличие доступа по локальной сети к базе данных ИКБ «КОДОС».

Установка модуля дизайна пропусков выполняется при инсталляции программы «Сервер ИКБ» или «Администратор ИКБ». Для этого необходимо отметить флагом соответствующий компонент (Рисунок 2.6).

Если модуль используется автономно на локальном компьютере, необходимо настроить связь с базой данных (см. п. Настройка подключения к базе данных).

SEC.RU | Короткий путь к информации Скачано с sec.ru

5 УСТАНОВКА КЛИЕНТСКИХ РАБОЧИХ МЕСТ

Клиентскими рабочими местами в ИКБ «КОДОС» являются автоматизированные рабочие места (АРМ), с установленными на них программами «Администратор ИКБ», «Мнемосхема», «Проходная», «Бюро пропусков». Подробнее узнать об установке, настройке и работе с программами можно в документах: «Руководство оператора программы „Мнемосхема“», «Руководство оператора программы „Проходная“», «Руководство оператора программы „Бюро пропусков“».

Все клиентские программы работают с базой данных, которая установлена на сервере ИКБ. Поэтому перед началом работы необходимо настроить доступ к базе данных с клиентского рабочего места (подробнее см. «Руководство оператора программы „Конфигуратор“»).

SEC.RU | Короткий путь к информации Скачано с sec.ru

6 КОНФИГУРИРОВАНИЕ ИКБ «КОДОС» ДЛЯ КРУПНЫХ ОБЪЕКТОВ

6.1 Настройка контроллеров с помощью утилиты ContrTools

ПРИМЕЧАНИЕ – Код ключа занимает в памяти контроллера 5 байт, запись о событии занимает 7 байт. При стандартном распределении памяти под коды ключей выделено 10200 байт (2040 ключей), снижать это значение не рекомендуется.

Конфигурирование ИКБ «КОДОС» для крупных объектов, где число карт доступа превышает 2000, заключается в дополнительной настройке параметров периферийного оборудования и ИКБ «КОДОС». В этом случае рекомендуется проводить перераспределение динамической памяти контроллеров доступа и параметров работы программы.

Чтобы избавиться от следов предыдущих конфигураций, в контроллере необходимо чистить память, выделяемую под коды ключей:

- при изменении объемов памяти, выделяемой для кодов ключей/ событий;
- при переносе контроллера, установке в новом месте;
- при подключении новых контроллеров.

Подробнее о процедуре очистки памяти контроллера и увеличении памяти, выделяемой под коды ключей см. «Руководство оператора программы „Настройка контроллеров“».

6.2 Использование локальных индексов

На крупных или территориально-распределенных объектах, объединенных общей базой данных, рекомендуется использовать эту функцию программы, если количество кодов карт пользователей, хранящихся в базе данных больше, чем позволяет записать память контролера.

Предполагается, что через конкретную точку доступа (дверь, турникет) одновременно не должен быть назначен доступ сразу всем пользователям из базы данных. При этом в память контроллера записываются коды карт только тех пользователей, которым разрешен доступ через точку или точки доступа, которыми управляет данный контроллер.

Программа хранит данные о картах, которые в данный момент находятся в контроллере. Когда через точку доступа впервые проходит новый пользователь, которому разрешен проход через неё, информация о его карте записывается на свободное место в памяти контроллера.

В случае если в памяти контроллера нет свободного места, устройство перезаписывает одну из существующих карт. Информация с этой карты, таким образом, удаляется из контроллера, но будет храниться в базе данных. Критерием выбора карты для замещения является наиболее давнее время прохода. Так, если в контроллере при добавлении новой карты недостаточно свободной памяти, из него будет удален код карты с наиболее давним временем прохода.

При проходе пользователя с картой, кода которой нет в памяти контроллера, происходит запрос о наличии этого кода в базе данных. Если код есть в базе, карта прописывается в память контроллера. С точки зрения пользователя, реакция контроллера при первом поднесении карты такая же, как и при поднесении неизвестной карты: считыватель будет мигать красным цветом. При повторном и любом последующем поднесении карты проход будет разрешён или запрещён согласно заданным владельцу карты в системе правам доступа.

Часть пользователей может быть всегда прописана в контроллерах. Такие карты никогда не перезаписываются новыми и всегда находятся в памяти контроллера. Чаще всего в этот список заносятся карты руководящего состава организации и сотрудников, отвечающих за поддержание систем жизнеобеспечения.

Для настройки локальных индексов во вкладке «Управление» → кнопка «Настройка системы» в разделе «Параметры сервера» следует установить флаг «Использовать локальные индексы» и настроить минимальный и максимальный локальный индексы (подробнее см. Настройка системы).

Перед включением функции локальных индексов необходимо провести перераспределение памяти контроллеров (см. «Руководство оператора программы „Настройка контроллеров“») с учетом максимального ее

SEC.RU | Короткий путь к информации Скачано с sec.ru

использования. Все контроллеры доступа в системе должны иметь одинаковые настройки распределения памяти. При включении функции локальных индексов параметр CriticalKeyIndex не используется.

6.2.1 Пример настройки

Например, существует организация (всего 15 000 сотрудников), имеющая головной офис в Москве (26 точек доступа) и 84 филиала по территории страны (по 2 точки доступа в каждом). В качестве контроллеров доступа используются контроллеры EC-202. В головном офисе находится сервер ИКБ «КОДОС», в каждом филиале установлено автоматизированное рабочее место (ПО «Администратор ИКБ»).

С помощью утилиты ContrTools следует перераспределить память всех (110 шт.) контроллеров доступа EC-202. Под коды ключей отводим максимально возможное значение — 51000 байт (10200 ключей), под события назначаем 7154 байт памяти (1022 события). Нужно помнить, что у контроллеров серии RC в два раза меньше памяти, поэтому при их использовании необходимо назначить следующие значения: 25500 байт под коды ключей, 3066 байт под события, что даст возможность хранить 5100 ключей и 432 события.

Пример настройки:

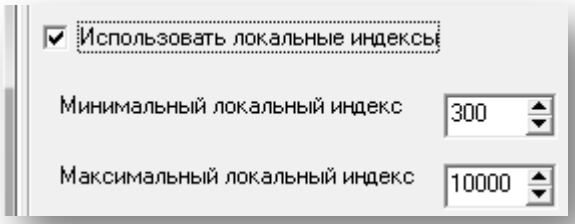


Рисунок 6.1

При запуске программы на вкладке «Пользователи» появится новая колонка «Позиция карты». У всех пользователей, карты которых заблокированы от удаления из памяти контроллера, значение в столбце «Позиция карты» выделено цветом.

При необходимости можно вручную регулировать привилегированные карты. Для исключения карты пользователя из списка привилегированных необходимо в карточке пользователя снять галочку в параметре «Поместить в начало списка». А для пользователя, чью карту необходимо заблокировать от удаления галочку нужно установить.

ПРИМЕЧАНИЕ – Функция локальных индексов работает только с СУБД Firebird.
Действия по блокировке\разблокировке карточки от удаления расцениваются программой как вновь выданные карты. Все события по этим пользователям, которые произошли ранее, будут недоступны.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

7 РАБОТА И ОБСЛУЖИВАНИЕ ПРОГРАММЫ

7.1 Логика обработки прохода пользователя

Пользователи идентифицируются по их кодоносителям при помощи считывателей. От считывателя в контроллер поступает код поднесенного кодоносителя. Номер считывателя (1 или 2) позволяет контроллеру определить, поднесен кодоноситель со стороны входа или выхода — в однодверном режиме работы, или же на входе какой из дверей (первой или второй) — в двухдверном режиме.

После приема кода от считывателя контроллер определяет соответствующие пользователю права и принимает решение о доступе. Если пользователю с этим кодом в данный момент времени доступ разрешен, то контроллер открывает замок двери, соответствующей считывателю, от которого принят код. Разрешение или запрет доступа определяют по цвету светодиода считывателя.

Права доступа в системе настраивают при помощи следующих параметров:

- таблица пользователей;
- уровень доступа;
- таблица уровней доступа;
- временные зоны;
- режим запрета повторного прохода;
- режим запрета выхода.

Контроллер доступа при принятии решения о разрешении прохода проверяет несколько условий.

Первое, необходимое для разрешения доступа, условие — это наличие кода кодоносителя в памяти контроллера. Если код контроллеру неизвестен (кодоноситель не прописан в памяти), то контроллер отказывает в доступе обладателю этого кодоносителя (сообщение — «на входе неизвестный код»).

Если код присутствует в памяти контроллера (кодоноситель прописан в памяти), то проверяется второе условие — наличие уровня доступа этого кодоносителя в таблице разрешенных уровней, действующих для данной двери в данный момент времени. Кодоносителю с уровнем доступа, отсутствующим в таблице разрешенных, контроллер в доступе отказывает (сообщение — «запрет входа»).

Уровень доступа — это число в диапазоне от 1 до 32, которое ставится в соответствие каждому коду кодоносителя, хранящемуся в памяти контроллера. В отличие от кода, уровень доступа не является собственной характеристикой кодоносителя, а задаётся при занесении кода в память контроллера и в дальнейшем может быть изменен. Коды кодоносителей вместе с соответствующими уровнями доступа заносятся в таблицу пользователей контроллера.

Третье условие, необходимое для разрешения доступа, — отсутствие ограничений по режиму запрета повторного прохода. Контроллер отказывает в доступе, если для считанного кодоносителя действует режим запрета повторного прохода (AntiPassBack) и в предыдущий раз проход с ним осуществлялся в том же направлении (событие – «попытка повторного входа»).

Режим запрета повторного прохода в одном направлении может быть включен или выключен. Когда режим запрета повторного прохода для какой-либо двери включен, два раза подряд входить или два раза подряд выходить с одним кодоносителем через эту дверь запрещается. Таким образом, пользователь сможет войти в дверь, только если ранее он из нее выходил, а выйти — только если ранее входил.

Когда режим AntiPassBack включен, ограничения действуют не для всех пользователей, а лишь для тех, чьи уровни доступа имеются в таблице запрета повторного прохода. Это позволяет выделить привилегированных пользователей (гостей, руководство) или тех сотрудников, у кого работа связана с частыми входами-выходами, чтобы избавить их от неудобств, вызванных необходимостью подносить кодоноситель к считывателю при каждом входе и выходе (даже если дверь уже открыта другим пользователем).

Когда кодоноситель подносится к считывателю ВЫХОД, то проверяется еще одно, четвертое условие — отсутствие запрета на выход для считанного кодоносителя. Режим запрета выхода может быть включен или выключен. Если он включен, то запрещается выход тем пользователям, уровни доступа которых находятся в таблице запрета выхода (сообщение-«запрос на выход»).

ПРИМЕЧАНИЕ – В программном обеспечении ИКБ «КОДОС» событие «Запрет выхода» трактуется как «Запрос на выход». Предполагается, что оператор (охранник), увидев сообщение о запросе на выход, может разблокировать дверь с компьютера, и тогда в системе будет зафиксировано событие «Выход с ключом пользователя, подносившего кодоноситель».

SEC.RU | Короткий путь к информации Скачано с sec.ru

Выполнения всех четырех описанных условий достаточно для разрешения доступа. Однако гибкость системы этим не исчерпывается: выполнение второго из условий зависит от момента времени, в который осуществляется попытка получения доступа.

Контроллер оперирует восемью временными зонами. Каждая временная зона состоит из восьми временных интервалов. Интервал считается активным, если выполнены два условия:

- текущий день недели отмечен флагом для данного интервала;
- текущее время («часы : минуты») попадает между началом и окончанием этого интервала.

Рассмотрим, например, интервал с 9:00 до 12:00, для которого установлены флаги Пн, Ср, Пт. Если сейчас 10:30 и сегодня среда, то данный интервал активен, если же сегодня вторник, то нет. Если в данный момент хотя бы один интервал временной зоны активен, то эта временная зона также считается активной.

С каждой временной зоной сопоставляется таблица уровней доступа. Если временная зона активна, то разрешены все уровни доступа, входящие в ее таблицу. Если в какой то текущий момент времени активны несколько временных зон, то текущая таблица доступа содержит все уровни доступа, разрешенные для активных временных зон в рассматриваемый момент времени.

Некоторое исключение из этого правила составляет доступ в праздничные дни. Флаг, соответствующий праздничным дням, перекрывает действие флагов, соответствующих дням недели.

Таким образом, если некоторый интервал активен, например, по средам, но не активен по праздникам, то он не активен в среду, являющуюся праздничным днем. Соответственно, уровни доступа, которые должны быть разрешены по средам, но не должны быть разрешены по праздникам, контроллер не считает разрешенными.

Если ни одна из временных зон в настоящий момент не активна, права доступа контроллер определяет по таблице доступа «по умолчанию». Та же таблица применяется, если режим использования временных зон для доступа отключен.

ПРИМЕЧАНИЕ – В двухдверном режиме работы контроллера уровень доступа пользователя одинаков для обеих дверей. Таблицы разрешенных уровней доступа для первой и второй дверей могут быть различными. Режимы запрета повторного прохода и запрета на выход при таком подключении контроллера должны быть отключены.

Нормальной считается последовательность событий, приведенная ниже:

- Пользователь подносит разрешенный кодоноситель к считывателю при закрытой двери.
- Контроллер фиксирует событие «Считывание ключа на входе (выходе)» и разблокирует замок (подаёт напряжение на клеммы, если замок прямого типа, или снимает, если инверсного) на время, заданное параметром «Длительность открытия замка».
- Пользователь открывает дверь в течение вышеуказанного интервала времени и проходит через нее. Обнаружив открытие двери (размыкание дверного датчика), контроллер фиксирует событие «Вход (выход) с ключом» пользователя с тем кодоносителем, который перед этим был считан.
- Пользователь закрывает дверь за время, не превышающее длительности открытия замка. Контроллер при этом фиксирует событие «Дверь закрыта».

Если время длительности открытия замка истекло, а дверь до этого момента не была закрыта, то контроллер фиксирует событие «Дверь оставлена открытой». Если открытия двери за период, равный времени длительности открытия замка, так и не произошло, то событие «Вход (выход) с ключом» не фиксируется, а замок остается разблокированным в течение данного интервала времени.

SEC.RU | Короткий путь к информации Скачано с sec.ru

7.1.1 Настройка прохода пользователя

Для выполнения прохода пользователю через дверь в программе ИКБ «КОДОС» необходимо, чтобы выполнялись следующие условия:

- наличие флажка рядом с описанием этой двери в поле «Разрешен доступ», в окне редактирования личных данных пользователя. Пока это условие не будет выполнено, сотрудник не сможет пройти через данную дверь, несмотря на другие настройки, дающие ему туда доступ.
- уровень доступа, назначенный пользователю, должен быть прописан как разрешенный в таблице доступа по временным зонам этой двери. Для настройки прохода пользователей по временным зонам следует нажать название временных зон и установить для каждой из них флажки для тех уровней доступа пользователей, которые должны иметь доступ через данную дверь в течение этой временной зоны.
- должна быть активна хотя бы одна временная зона, в которой разрешен уровень доступа, назначенный этому пользователю.
- срок действия карты пользователя на данный момент не истек.

Организация проходов посетителей (гостей)

- Определить специальный уровень доступа для гостевых карт. Например, если сотрудники имеют уровень доступа «1», то для гостевых карт установить уровень доступа «2». Этот уровень доступа должен быть уникальным и не использоваться другими сотрудниками.
- Для дверей, через которые можно проходить с гостевыми картами, установить разрешенный уровень доступа (например, «2») — поставить флажок у номера уровня доступа. Для других уровней доступа флажки менять не требуется (Рисунок 7.1).

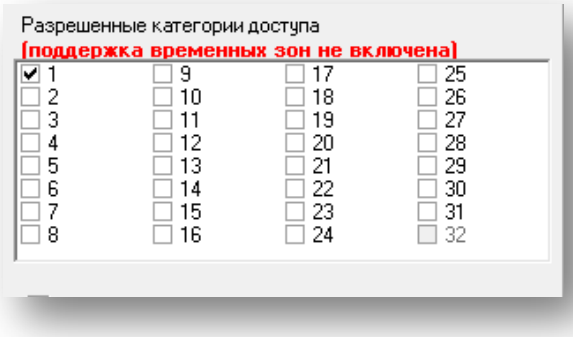


Рисунок 7.1

- Если требуется, чтобы выход по гостевым картам происходил через одну дверь, необходимо задать ограничения, нажав кнопку «По уровням доступа» в окне «Настройка двери». После чего появится окно «Дополнительные ограничения доступа». В этом окне для уровня доступа гостей (например, «2») установить флажок: «Запретить выход через эту дверь». Кроме того, необходимо установить контроль ограничения выхода — установить флажок «Ограничение выхода» в окне «Настройка двери». Ограничение выхода необходимо применять, в основном, для сохранности кодоносителей. При использовании картоприемника возвращение кодоносителей пользователями происходит автоматически.
- Действия п. 2 – 4 выполнить для всех временных зон выбранной двери.

SEC.RU | Короткий путь к информации Скачано с sec.ru

7.2 Обслуживание базы данных

Для поддержания высокой надежности и оперативности работы используемой СУБД необходимо проводить периодическое обслуживание базы данных. Рекомендуется с периодичностью, определяемой пользователем, проводить выгрузку событий из базы данных, проверку и резервное копирование БД. При обнаружение ошибок восстанавливать БД из резервной копии.

Периодичность проведения данных действий выбирается, исходя:

- из размера системы на объекте;
- количества пользователей (карт доступа), зарегистрированных в системе;
- интенсивности использования системы.

7.2.1 Выгрузка событий из БД

В ИКБ «КОДОС» существует возможность проводить:

- выгрузку событий из базы данных и сохранение выборки в виде отдельного файла;
- удалять из архива текущие события;
- удалять из архива выбранные события.

Для того чтобы выгрузить события из БД, необходимо:

1. Во вкладке «События в системе» нажать кнопку «Архив событий». В появившемся окне «Архив событий» нажать кнопку «Архив». В списке выбрать «Выгрузить архив» (Рисунок 7.2).

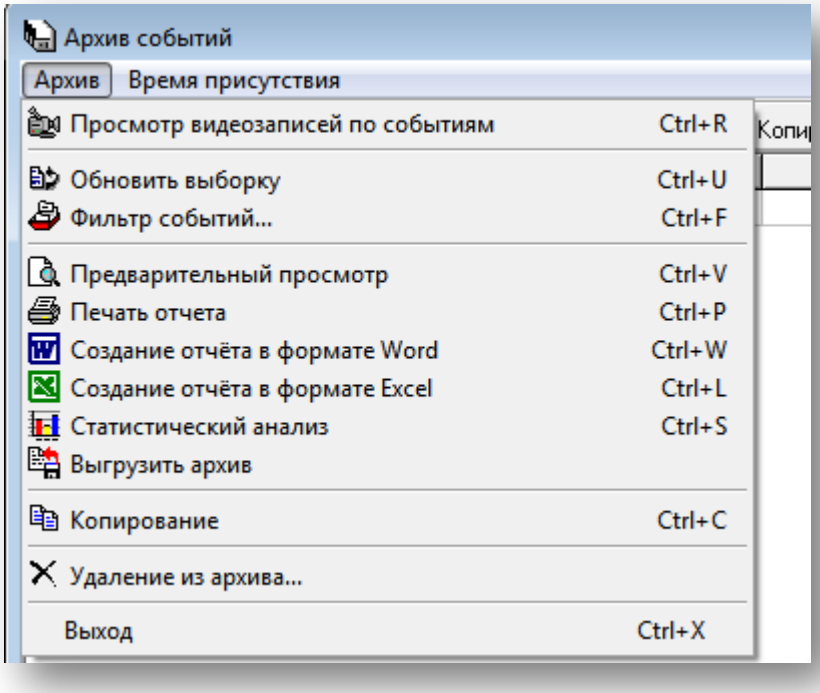


Рисунок 7.2

2. В окне «Выгрузка архива» (Рисунок 7.3) в разделе «Период» задать период выгружаемого архива. В разделе «Действия над таблицами» выбрать «Создать и перенести». В строке «Описание» задать имя выгружаемого файла.

SEC.RU | Короткий путь к информации Скачано с sec.ru

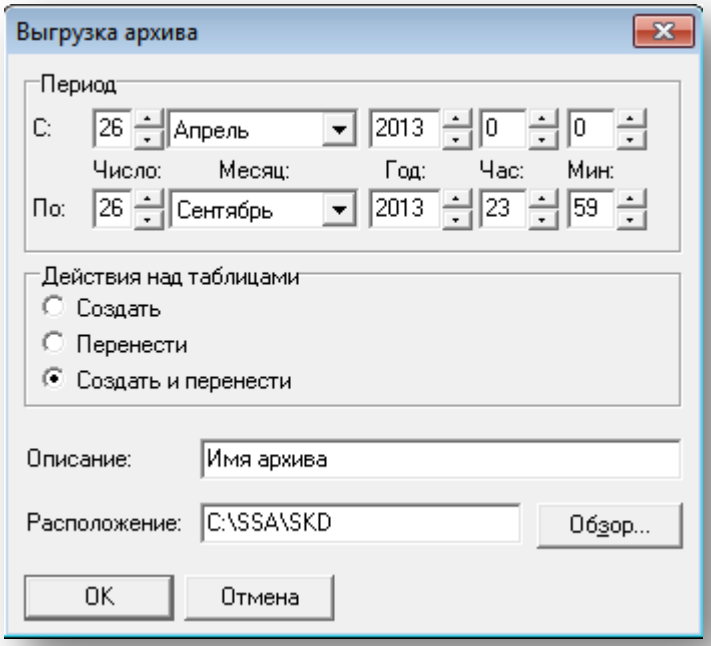


Рисунок 7.3

3. В строке «Расположение» указать, куда сохранить указанный файл. Для этого нажать кнопку «Обзор» и в появившемся окне «Обзор папок», (Рисунок 7.4) выбрать место сохранения файла. После указания места сохранения нажать кнопки «ОК».

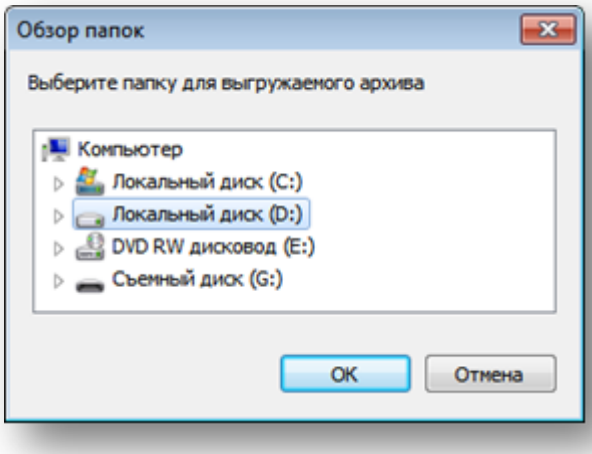


Рисунок 7.4

4. Начнется процесс выгрузки архива (Рисунок 7.5).

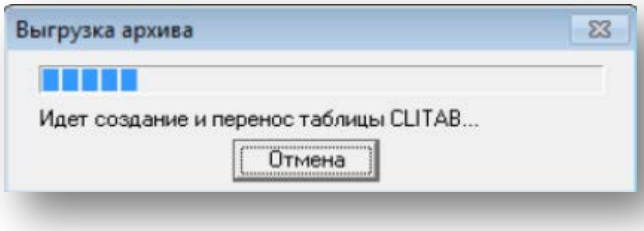


Рисунок 7.5

5. Выгруженный архив можно просмотреть в программе MS Access или аналогичной. После окончания процесса выгрузки архива будет предложено удалить выгруженный архив из СУБД. Нажать кнопку «Да» (Рисунок 7.6).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

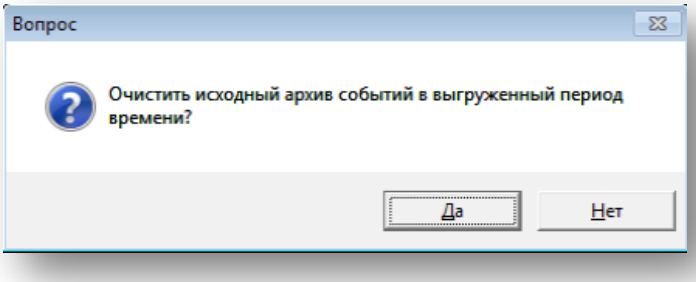


Рисунок 7.6

6. Архив будет удален из СУБД, появится уведомление (Рисунок 7.7). Нажать «ОК».

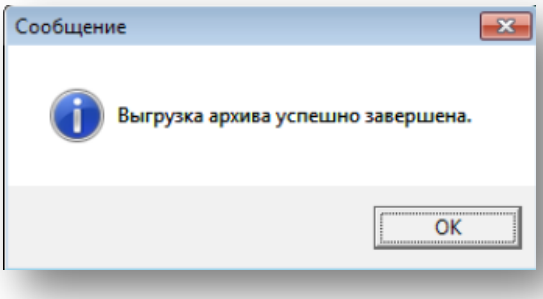


Рисунок 7.7

7. После выгрузки событий рекомендуется провести процедуры резервного копирования и восстановления БД.

7.2.2 Проверка, копирование и восстановление БД

Проверка, резервное копирование и восстановление базы данных должны выполняться сотрудниками, имеющими представление о работе СУБД, используемой в данной системе.

ВНИМАНИЕ! Перед проведением копирования необходимо обязательно отключать все автоматизированные рабочие места (АРМ) системы, работающих с базой данной и отключить программу «Сервер ИКБ», чтобы к рабочей базе данных не было обращений, иначе при копировании может быть получен испорченный файл базы.

ИКБ «КОДОС» поддерживает работу следующих СУБД: Firebird, Oracle и MS SQL.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

8 ПРИЛОЖЕНИЕ «А». Глоссарий

Администратор системы — специалист, выполняющий установку, настройку и техническое обслуживание системы. Имеет наивысший приоритет доступа в системе.

Активный элемент экранной формы — текущий, выделенный элемент.

Артефакты — искажения изображения, звука.

Архив видеоканала — файлы с записанной видео- и аудиоинформацией, элемент дерева конфигурации видеоканалов.

Видеоархив — запись видеоизображений хранящихся в памяти компьютера.

Видеоканал — оборудование (плата видеоввода, мультиплексор, сеть), являющееся источником видеосигнала, а также элемент древовидной структуры, служащий для настройки соответствующего оборудования.

Видеоокно — окно, в котором отображается видеоинформация.

Деинсталляция — удаление программного обеспечения.

Детектор движения — программный модуль, включающий видеозапись при обнаружении движения.

Дочерний элемент — подчиненный элемент в дереве каталога.

Инсталляция — установка программного обеспечения.

Клиент — компьютер и ПО, принимающее информацию по локальной сети от сервера.

Ключ аппаратной защиты — устройство, предназначенное для защиты программы на аппаратном уровне от несанкционированного копирования и эксплуатации.

Кодек — кодировщик/ декодировщик данных.

Кольцевая запись — способ записи, когда новая запись замещает старую.

Коммутация аудиоканала — включение звукового сопровождения изображения, поступающего с видеоканала.

Контекстное меню — меню, вызываемое щелком правой клавиши мыши.

Контекстная справка — раздел справочной системы программы.

Конфигурация архивов — настройка видеоархивов. Для каждой конфигурации каналов ПК может быть сформирована только одна конфигурация архивов.

Конфигурация видеоокон — элемент конфигурации видеоокон (каналов и архивов). Для каждой конфигурации каналов ПК может быть сформировано несколько различных конфигураций видеоокон. В каждый момент времени только две из них являются текущими: одна для основного окна программы, другая — для окна «Видеоархивы».

Конфигурирование каналов ПК — выполненные на компьютере системы настройки видеоканалов, конфигурации видеоокон, конфигурация архивов, настройки панелей инструментов и др. Для каждого ПК может быть сформировано несколько различных конфигураций каналов. В каждый момент времени только одна является текущей.

Конфигурация системы — оборудование, интерфейс и настройки устройств, входящих в состав системы.

Корневой элемент — первый элемент в дереве элементов, все остальные элементы для него являются дочерними.

ЛВС — локальная вычислительная сеть.

Лицензия — право на использование компонентов системы.

Менеджер лицензий — программа, предназначенная для активизации модулей ПО в соответствии с лицензией.

Мультиплексор — электронное устройство, переключающее видеоканалы; тип видеоканала.

Название видеоканала — идентификатор (имя) видеоканала.

Оператор — Пользователь системы.

Главное (верхнее) меню — меню (обычно располагается сразу под заголовком окна программы), где собраны все основные команды, выполняемые программой.

Панель видеоокна — образ, служащий для задания положения и размеров видеоокон при конфигурировании.

Панель инструментов — экранная форма, служащая для размещения кнопок, полей ввода и т. п., предназначенных для выполнения определенных функций программы.

Пароль пользователя — запись, служащая для идентификации пользователя.

Период обновления видеоканала — промежуток времени, по прошествии которого система обновляет связь с источником видеосигнала.

ПК — персональный компьютер.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Пиксель — минимальная единица изображения на экране монитора. В записи «384x288» первое число означает число точек по горизонтали, второе — по вертикали.

Планировщик — программный модуль для управления автоматическим включением/ выключением записи по расписанию.

Плата видеоввода — устройство видеозахвата; тип видеоканала.

Пользователь — оператор, осуществляющий работу с программным обеспечением. Идентифицируется при помощи ввода имени и пароля.

Предтревожная запись — режим, позволяющий включать в видеозапись некоторое число кадров, предшествующих тревоге.

Рабочая директория программы — место размещения загрузочного модуля программы и других вспомогательных файлов.

Рабочая область окна — часть окна программы, внутри которой располагаются вторичные окна.

Разрядность — параметр, характеризующий число различаемых уровней.

Регистрация пользователя — вход в систему путем ввода имени и пароля пользователя.

Сеть — несколько компьютеров и средства их связи; тип видеоканала.

Сетевая камера — сетевое устройство видеоввода, тип видеоканала.

Сервер — компьютер, к которому подключено оборудование системы, и соответствующее ПО, управляющее работой этого оборудования.

Система — совокупность оборудования и программного обеспечения «ИКБ КОДОС».

СКУД — система контроля и управления доступом.

Тип видеоканала — либо плата видеоввода, либо мультиплексор, либо сеть.

Текущий объект (окно, конфигурация и др.) — активный объект, с которым работает оператор. В списке аналогичных ему элементов обычно выделяется цветом, фоном.

Текущий пользователь — пользователь, зарегистрированный по определенному имени и паролю и управляющий работой компьютера.

Устройство аудиозахвата — устройство ввода звуковой информации.

Устройство аудиовоспроизведения — устройство вывода звуковой информации.

Частота дискретизации — количество минимальных единиц (дискрет) в единицу времени при преобразовании аналогового сигнала в цифровой.

Шум — неинформативная часть сигнала, отделяемая от информативной части с помощью фильтров.

SEC.RU | Короткий путь к информации
Скачано с sec.ru