

В. Т. Корниенко

**ОСНОВЫ ПОСТРОЕНИЯ
РАДИОЭЛЕКТРОННЫХ ПОДСИСТЕМ
КОМПЛЕКСНЫХ СИСТЕМ
БЕЗОПАСНОСТИ**

Учебное пособие

**Ай Пи Эр Медиа
Саратов • 2018**

УДК 681.5
ББК 32.84
К67

Автор:

Корниенко В. Т. — доцент кафедры РТС
Института радиотехнических систем и управления
Южного федерального университета

Рецензенты:

Макаров А. М. — доктор технических наук, профессор
Северо-Кавказского федерального университета;
Федоров В. М. — кандидат физико-математических наук, доцент
Южного федерального университета

Корниенко, В. Т.

К67 Основы построения радиоэлектронных подсистем комплексных систем безопасности [Электронный ресурс] : учебное пособие / В. Т. Корниенко. — Электрон. дан. и прогр. (11 Мб). — Саратов: Ай Пи Эр Медиа, 2018. — 140 с.

ISBN 978-5-4486-0589-5

Рассмотрены вопросы построения таких подсистем комплексных систем безопасности как охранно-пожарная сигнализация, контроль и управление доступом и видеонаблюдение. Приведены варианты их конфигурирования и проектирования на примерах оборудования известных производителей.

Предназначено для студентов радиотехнических специальностей для изучения разделов дисциплин «Технические средства охраны», «Технические средства защиты информации».

Учебное электронное издание

© Корниенко В. Т., 2018
© ООО «Ай Пи Эр Медиа», 2018

Издано в авторской редакции

Технический редактор, компьютерная верстка *А.Д. Матлахова*
Обложка *С.С. Сизиумовой*

Для создания электронного издания использовано:
Приложение pdf2swf из ПО Swftools, ПО IPRbooks Reader,
разработанное на основе Adobe Air

Подписано к использованию 16.11.2018. Объем данных 11 Мб.

Издание представлено в электронно-библиотечных системах
IPR BOOKS (www.iprbookshop.ru),
Библиокомплектатор (www.bibliocomplectator.ru)

Бесплатный звонок по России: **8-800-555-22-35**
Тел.: 8 (8452) 24-77-97, 8 (8452) 24-77-96

Отдел продаж и внедрения ЭБС:
доб. 206, 213, 144, 145
E-mail: sale@iprmedia.ru

Отдел комплектования ЭБС:
доб. 224, 227, 208
E-mail: mail@iprbookshop.ru

По вопросам приобретения издания обращаться:
доб. 208, 201, 222, 224
E-mail: izdat@iprmedia.ru, author@iprmedia.ru

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....	6
1. КОНФИГУРИРОВАНИЕ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА «PERCO» С БЕСОНТАКТНЫМИ СЧИТЫВАТЕЛЯМИ ПЛАСТИКОВЫХ КАРТ И БИОМЕТРИЧЕСКИМИ СЧИТЫВАТЕЛЯМИ ОТПЕЧАТКОВ ПАЛЬЦЕВ	8
1.1. Цель	8
1.2. Краткие теоретические сведения	8
1.2.1. Аппаратное обеспечение СКУД	8
1.2.2. Программное обеспечение СКУД	23
1.2.3. Порядок работы контроллера PERCo-SC-610T/L при управлении одним замком.....	47
1.3. Экспериментальное задание	53
1.4. Контрольные вопросы	54
2. ПРОЕКТИРОВАНИЕ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ С ПОМОЩЬЮ ПРОГРАММЫ VIDEOCAD	55
2.1. Цель	55
2.2. Краткие теоретические сведения	55
2.2.1. Сравнительный анализ камер охранного видеонаблюдения.....	55
2.2.2. Основы работы в VideoCAD	62
2.3. Экспериментальное задание	77
2.4. Контрольные вопросы	77
3. ИЗУЧЕНИЕ ОСНОВНЫХ ХАРАКТЕРИСТИК БЕСПРОВОДНОЙ ОХРАННОЙ СИГНАЛИЗАЦИИ «OASIS» ...	78
3.1. Цель	78
3.2. Краткие теоретические сведения	78
3.3. Экспериментальное задание	103
3.4. Контрольные вопросы	104

4. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ИНТЕГРИРОВАННОЙ СИСТЕМЫ ОХРАНЫ «ОРИОН»	105
4.1. Цель	105
4.2. Краткие теоретические сведения	105
4.3. Экспериментальное задание	137
4.4. Контрольные вопросы	138
 ЛИТЕРАТУРА	 139

ВВЕДЕНИЕ

Предлагаемое учебное пособие необходимо для усвоения материала, преподаваемого по дисциплинам «Охранные радиоэлектронные системы», «Технические средства охраны», «Технические средства защиты информации». В основу пособия положены основы построения основных подсистем комплексных систем безопасности объектов.

Для успешного усвоения разделов дисциплины необходимы знания, полученные студентами при изучении предшествовавших дисциплин, касающихся высшей математики, информатики, теории электросвязи, цифровых устройств. Материал пособия будет полезен при подготовке выпускных квалификационных работ бакалавров и специалистов.

Цель предлагаемого учебного пособия:

- освоить принципы построения и настройки систем контроля доступа на основе контроллеров Perco-SC-600 с биометрическими считывателями BioTrax;
- освоить создание проекта системы видеонаблюдения на основе трехмерной модели объекта с помощью программы VideoCad;
- ознакомиться с составом оборудования и принципом настройки беспроводной системы охранной сигнализации Оазис;
- ознакомиться с составом оборудования интегрированной системы охраны Орион и изучить возможности конфигурирования системы.

При решении задач анализа рассмотренных подсистем определяются основные показатели эффективности их функционирования, которые рассмотрены в отдельных подразделах. Для проведения исследований используются радиоэлектронные устройства подсистем охранно-пожарной сигнализации и контроля и управления доступом, а также персональный компьютер, программное обеспечение Perco-SC-600, BioTrax, АРМ Орион и среда графического проектирования VideoCAD, используемая компанией CCTV.

В первом разделе изложены принципы построения и настройки систем контроля доступа на основе контроллеров Perco-SC-600 с биометрическими считывателями BioTrax. Второй раздел посвящен основам создания проекта системы видеонаблюдения на основе трехмерной модели объекта с помощью программы VideoCad. Третий раздел пособия позволит ознакомиться с составом оборудования беспроводной системы охранной сигнализации Оазис и изучить возможности ее центрального блока — приемно-контрольного прибора. В четвертом разделе изложены основы построения интегрированной системы безопасности Орион, характеристики основного оборудования системы и возможности ее конфигурирования.

Известно много учебных пособий по основам построения систем безопасности [1–7]. В данном учебном пособии используется известные данные, взятые за основу из многих источников при работе с перечисленным оборудованием систем охраны, а также приведены оригинальные решения, применяемые в учебном процессе.

Для успешного освоения преподаваемых дисциплин в учебное пособие включен набор экспериментальных заданий для выполнения на действующем лабораторном оборудовании охранных систем. При отсутствии реального оборудования для практического освоения работы возможно использовать программное обеспечение рассмотренных производителей систем безопасности — все это стирает традиционные препятствия при проектировании подсистем комплексных систем безопасности. Это позволяет расширять границы лабораторного эксперимента, строя его в виде виртуального конструктора.

1. КОНФИГУРИРОВАНИЕ СИСТЕМЫ КОНТРОЛЯ ДОСТУПА «PERCO» С БЕСОНТАКТНЫМИ СЧИТЫВАТЕЛЯМИ ПЛАСТИКОВЫХ КАРТ И БИОМЕТРИЧЕСКИМИ СЧИТЫВАТЕЛЯМИ ОТПЕЧАТКОВ ПАЛЬЦЕВ

1.1. Цель

Исследовать принципы построения и настройки систем контроля доступа на основе контроллеров Perco-SC-600 с биометрическими считывателями BioTrax.

1.2. Краткие теоретические сведения

1.2.1. Аппаратное обеспечение СКУД

Системы контроля и управления доступом имеют сетевую структуру по топологии общей шины [6, 7] и один из вариантов построения сети контроллеров поддерживает интерфейс RS-485. Оборудование может быть сконфигурировано и работать как в автономном режиме, так и быть настроено под управлением специализированного ПО, установленного на компьютере и управляться по сети.

Система позволяет организовать пропуск сотрудников на предприятие и отдельные помещения, осуществляя идентификацию по бесконтактным картам доступа по принципу «свой-чужой» и регистрируя время прохода. Сотрудникам и посетителям могут задаваться индивидуальные права доступа на объекты. Доступ может разграничиваться:

- **по времени**, т.е. каждому сотруднику задается индивидуальный временной график доступа на объект. В случае попытки прохода сотрудника вне установленных временных рамок доступа, система не пропустит его, фиксируя при этом время попытки прохода;

- **по статусу**, т.е. для каждого сотрудника можно определить объекты, на которые он имеет право доступа и право постановки/снятия на охрану. Система позволяет запретить двойной проход в одну сторону через турникет, что решает проблему с передачей пропуска другому человеку. В системе предусмотрена многоуровневая идентификация сотрудника: организация доступа при условии «карта + набор кода».

На любом из объектов может быть организован режим видеонаблюдения, когда право доступа реализуется только с подтверждения охранника после сравнения им полученного от видеокамеры изображения лица, предъявившего карту доступа, с эталонным изображением владельца карты доступа, хранящимся в системе.

В системе предусмотрен специальный режим «Охрана». В режиме «Охрана» попасть на объект могут лишь сотрудники, обладающие правом снятия/постановки объекта на охрану, что позволяет разделить сотрудников на иерархические группы в зависимости от прав доступа.

Система дает возможность получить информацию об учете рабочего времени любого сотрудника на любой части подконтрольной территории, в частности, на рабочем месте. На основе регистрируемых событий система позволяет получать следующие отчеты как для каждого сотрудника отдельно, так и для группы сотрудников:

- время присутствия на рабочем месте;
- контроль прихода на работу ранее установленного времени;
- контроль задержки на работе;
- контроль отсутствия выхода;
- опоздания на работу;

- уход с работы раньше времени;
- отсутствующие;
- общий отчет по всем нарушениям.

Система обеспечивает **автоматизированный кадровый учет, оформление и выдачу пропусков.**

В состав технических средств СКУД может входит следующее оборудование:

- сетевой контроллер;
- считыватель бесконтактных пластиковых карт;
- биометрический считыватель/контроллер;
- электромагнитный замок;
- кнопка выхода;
- преобразователь интерфейса RS-485/RS-232;
- резервный источник питания и др.

Специализированное программное обеспечение включает в себя ПО PERCo-S-600 и ПО BioTrax.

Учебно-лабораторный стенд на 2 точки прохода, реализованный на кафедре БИТ ТТИ ЮФУ имеет общую структуру, приведенную на рис. 1.1: для удобства занесения кодов карт пользователей и их биометрических данных требуется наличие у компьютера нескольких последовательных портов, в данном случае 4: один — для настольного считывателя, один — для конвертера интерфейсов от контроллера для дверного считывателя и два — для конвертера интерфейсов от биометрических считывателей BioTraks. Наличие же у компьютера одного СОМ-порта требует перед каждым подключением оборудования к порту производить выключение и перезагрузку компьютера.

Как видно из рис. 1.1, сетевая структура СКУД обеспечивается контроллерами фирмы-производителя Perco, а в качестве демонстрации биометрических считывателей системы использовано оборудование фирмы Rosslare. Поэтому вначале рассмотрим последовательно используемое аппаратное обеспечение, а затем его конфи-

гурирование как с помощью программного обеспечения, установленного на компьютере, так и с помощью встроенного программного обеспечения, позволяющего настраивать работоспособность оборудования в автономном режиме без подключения к компьютеру.

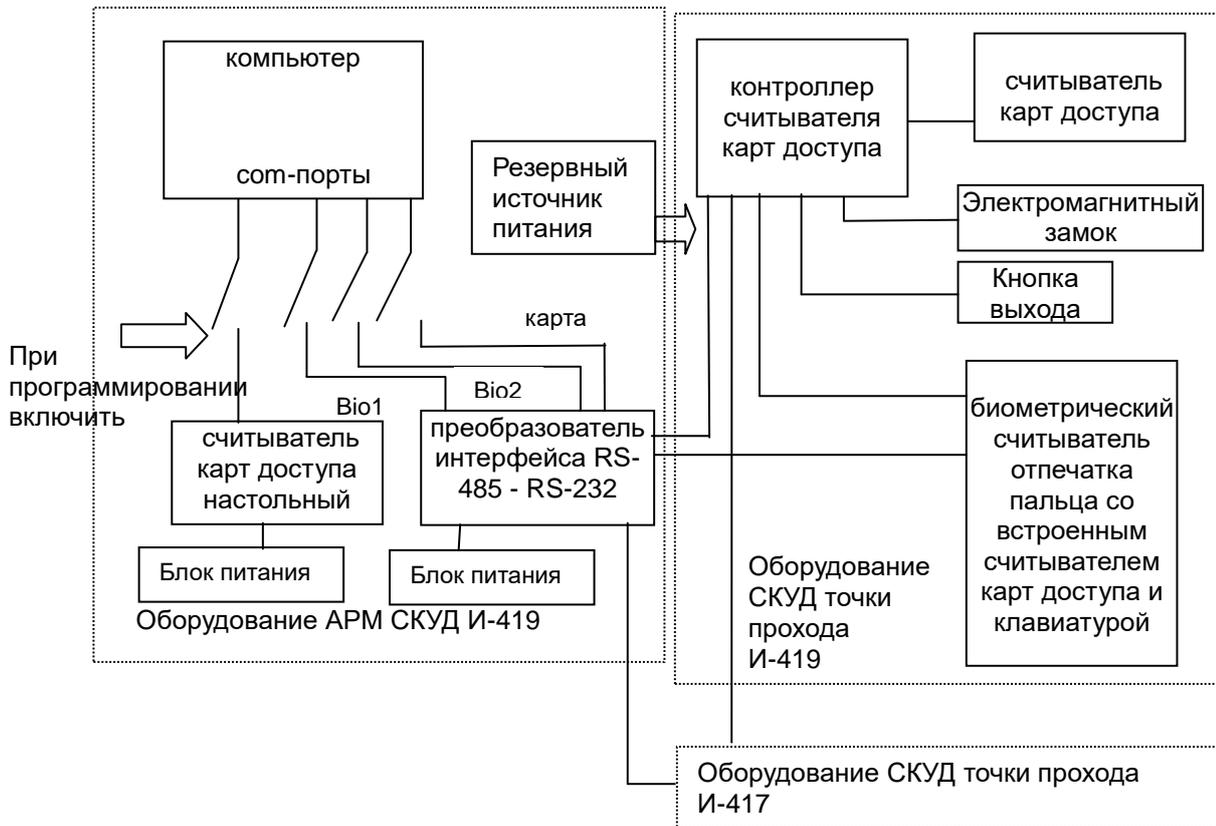


Рис. 1.1. Обобщенная структурная схема СКУД на две точки прохода

Оборудование системы контроля доступа Perco 600-й серии является сетевым, поддерживающим протокол RS-485, то все сетевое подключение оборудования имеет топологию общей шины, как показано на рис. 1.2. Для подключения к компьютеру используется преобразователь интерфейса RS-485 /RS-232, функциональная схема подключений которого приведена на рис. 1.3. Внешний вид платы контроллера замка на два считывателя карт приведен на рис. 1.4 [2].



Рис. 1.2. Структурная схема соединения контроллеров замка в общую шину и подключения к компьютеру через преобразователь интерфейса

Для организации входа и выхода в помещении по бесконтактным картам доступа допускается использование двух контроллеров замка одновременно при управлении одним замком (если модификация контроллера замка предусматривает использование одного считывателя карт).

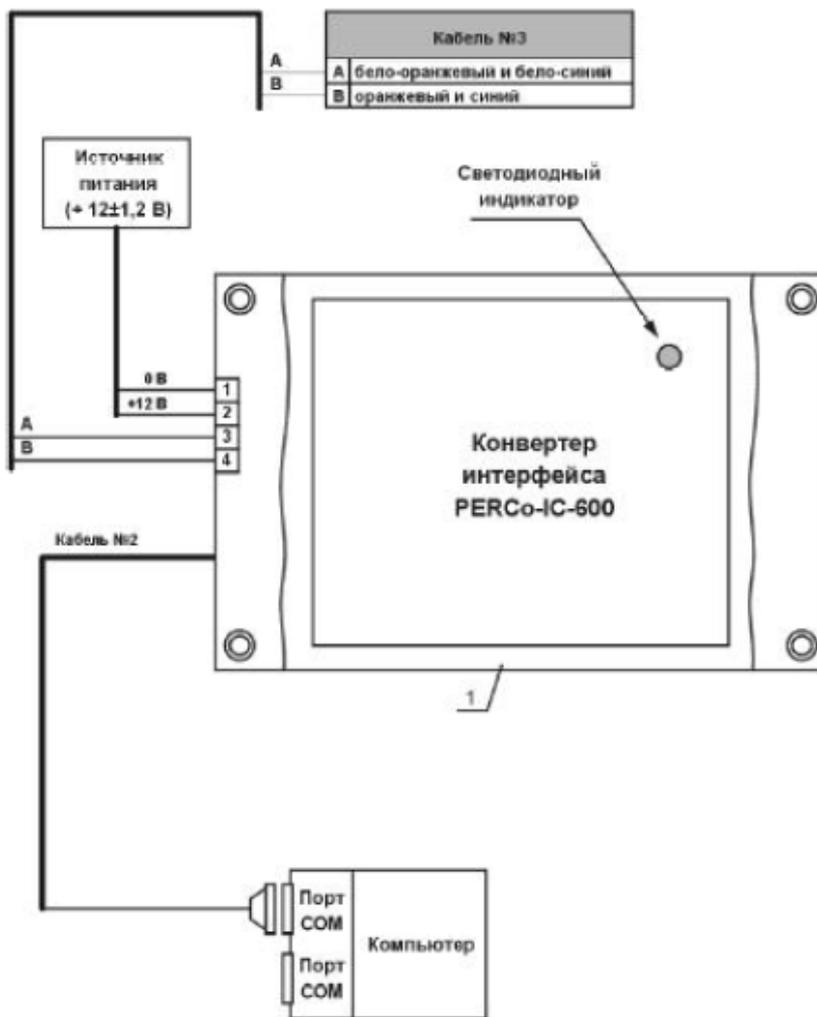


Рис. 1.3. Функциональная схема подключения преобразователя интерфейса RS-485/RS-232

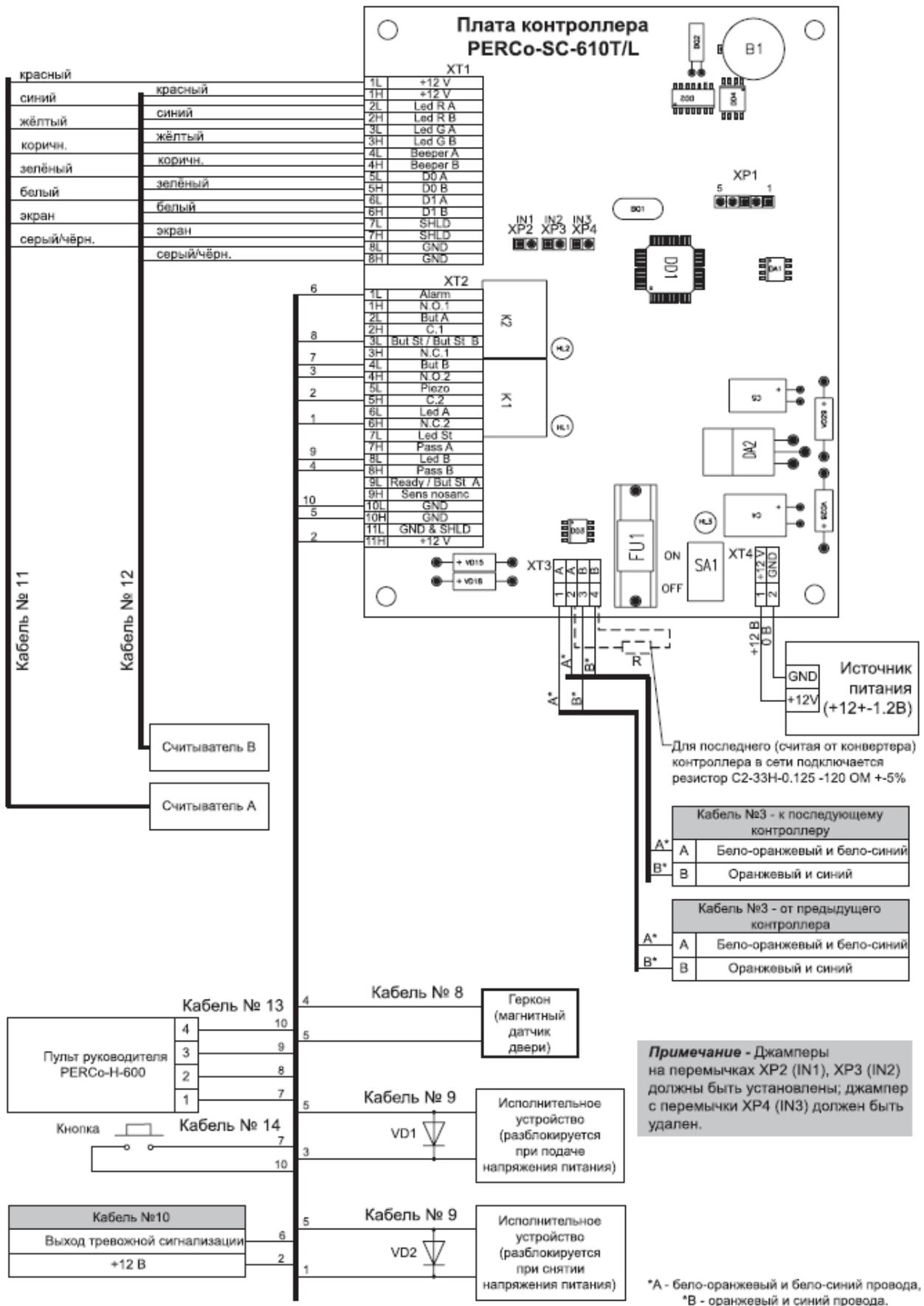


Рис. 1.4. Внешний вид платы контроллера замка на два считывателя карт

Для предотвращения пригорания контактов реле, используемого для включения исполнительного устройства и устранения радиопомех, необходимо использовать искрогасящие диоды, подбираемые исходя из рабочего напряжения конкретного исполнительного устройства (замка) и его потребляемого тока (например, для напряжения 12 В и рабочего тока 0,3 А необходим диод с обратным напряжением больше 12 В и прямым током 0,1–1 А). Могут использоваться замки, срабатывающие либо при подаче на него напряжения питания, либо при снятии с него напряжения питания. При использовании замков с импульсным управлением питание замка осуществляется от отдельного источника.

Технические характеристики контроллера приведены в табл. 1.1.

Таблица 1.1

Технические характеристики PERCo-SC-610T/L

Параметр	Значение
Количество пользователей	
- в режиме «Замок», «Два замка»	1000
- в режиме «Турникет»	2000
Энегрoneзависимая память, событий	
- в режиме «Два замка»	950
- в режиме «Замок», «Турникет»	2000
Выходной интерфейс	Wiegand 26
Стандарт карт	EM-Marine, HID
Количество поддерживаемых считывателей	2
Тип выхода	открытый коллектор
Интерфейс связи с конвертером интерфейса	RS-485
Время удержания в открытом состоянии, с	1 ÷ 255
Напряжение питания, В	12
Ток потребления, А	0,15

Конвертер интерфейса PERCo-IC-600 служит для подключения сетевых контроллеров к персональному компьютеру и согласует стандартные интерфейсы RS-485: (два провода) и RS-232: (четыре провода). Основные характеристики преобразователя интерфейсов приведены в табл. 1.2.

Считыватель бесконтактный PERCo-RP-14MW предназначен для использования в системах идентификации, контроля доступа и т.п. Считыватели обеспечивают считывание кода с идентификаторов Proximity с рабочей частотой 125 кГц OEM форматов Wiegand W26...W37 со стандартной организацией кодированного сигнала карты), а также производства EM-Microelectronic-Marin SA и «Ангстрем» (см. рис. 1.5).

Таблица 1.2

Технические характеристики преобразователя интерфейсов

Параметр	Значение
Максимальное число контроллеров, подключаемых к интерфейсу RS-485	64
Скорость передачи данных, бод	19200
Расстояние между конвертером и компьютером, м	не более 15
Расстояние между конвертером и контроллерами, м	не более 1200
Напряжение питания постоянного тока, В	12±1,2
Ток потребления, А	не более 0,06

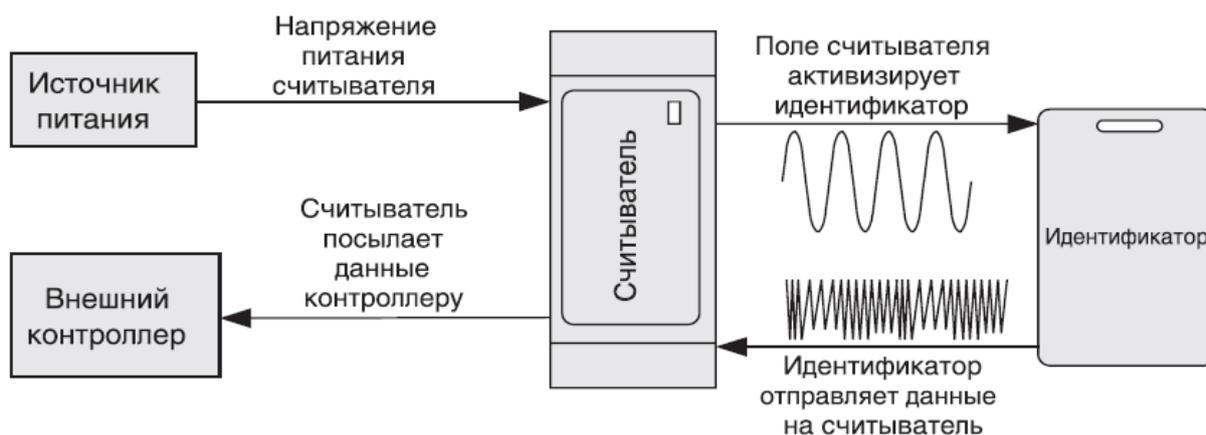


Рис. 1.5. Структура взаимодействия считывателя с идентификатором и контроллером

Каждый идентификатор имеет свой персональный код (количество комбинаций — более 500 млрд), который определяется однократно на этапе изготовления и не может быть изменен в процессе эксплуатации. Идентификаторы не имеют встроенного источника питания, что делает их срок службы практически неограниченным.

Считывание кода происходит при поднесении идентификатора к считывателю, для карточек на расстояние 10 см, для брелоков на расстояние 5 см. При этом идентификатор может находиться в кармане, в бумажнике или в любом другом магнитопрозрачном футляре. Предельное расстояние, на котором считывателем обеспечивается считывание идентификаторов, зависит от типа идентификатора.

Во включённом состоянии считыватель излучает вблизи себя низкочастотное (125 кГц) электромагнитное поле. Идентификатор, оказываясь в этом поле, активизируется и начинает передавать индивидуальный кодированный сигнал, принимаемый считывателем. Данные передаются внешнему контроллеру однократно, асинхронно, в момент первого достоверного приема сигнала от идентификатора. Повторная передача данных возможна не ранее чем через 200 мс после выхода идентификатора из зоны устойчивого приема.

Для передачи используются два провода «данные 0» и «данные 1». Появление логического уровня «0» на одном из проводов сигнализирует о наличии в кодовой посылке бита с соответствующим значением.

Длина кодовой посылки зависит от выбранного при монтаже режима и может быть либо фиксированной, либо определяться размером данных полученных от идентификатора.

При отличии длины кодовой посылки, принятой от идентификатора, от длины выходной кодовой посылки действуют следующие правила:

1. Если принятая от идентификатора кодовая посылка длиннее выходной, отбрасываются лишние старшие разряды.

2. Если принятая от идентификатора кодовая посылка короче выходной, недостающие старшие разряды заполняются нулями.

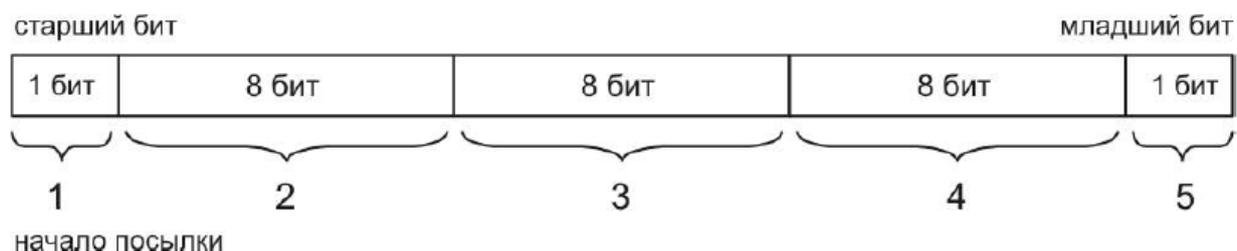


Рис. 1.6. Структура кодовой посылки в формате Wiegand 26

Данные передаются старшими битами вперед. Структура кодовой посылки для форматов фиксированной длины представлены на рис. 1.6, на котором обозначены группы бит следующим образом:

1 — контрольный бит (соответствует паритету на чётность для следующих 12 бит данных).

2 — байт кода семейства.

3 — старший байт номера карточки.

4 — младший байт номера карточки.

5 — контрольный бит (соответствует паритету на нечётность для предыдущих 12 бит данных).

Все байты передаются старшими битами вперед.

Временные характеристики выходного формата данных: длительность информационного импульса — 100 мкс, период повторения импульсов — 1 мс.

Считыватель имеет звуковую и светодиодную индикацию и может быть переключен в один из двух вариантов управления светодиодной индикацией: «double line» — управление по двум линиям, и «single line» управление по одной линии.

Считывание кода подтверждается считывателем кратковременным включением на его корпусе зеленого светодиода индикатора (в варианте «double line») или кратковременным переключением цвета светодиода индикатора с красного на зеленый (в варианте «single line»). Для включения варианта управления «single line» необходимо, до подачи питания на считыватель, подать сигнал низкого уровня на оранжевый провод соединительного кабеля (см. рис. 1.7).

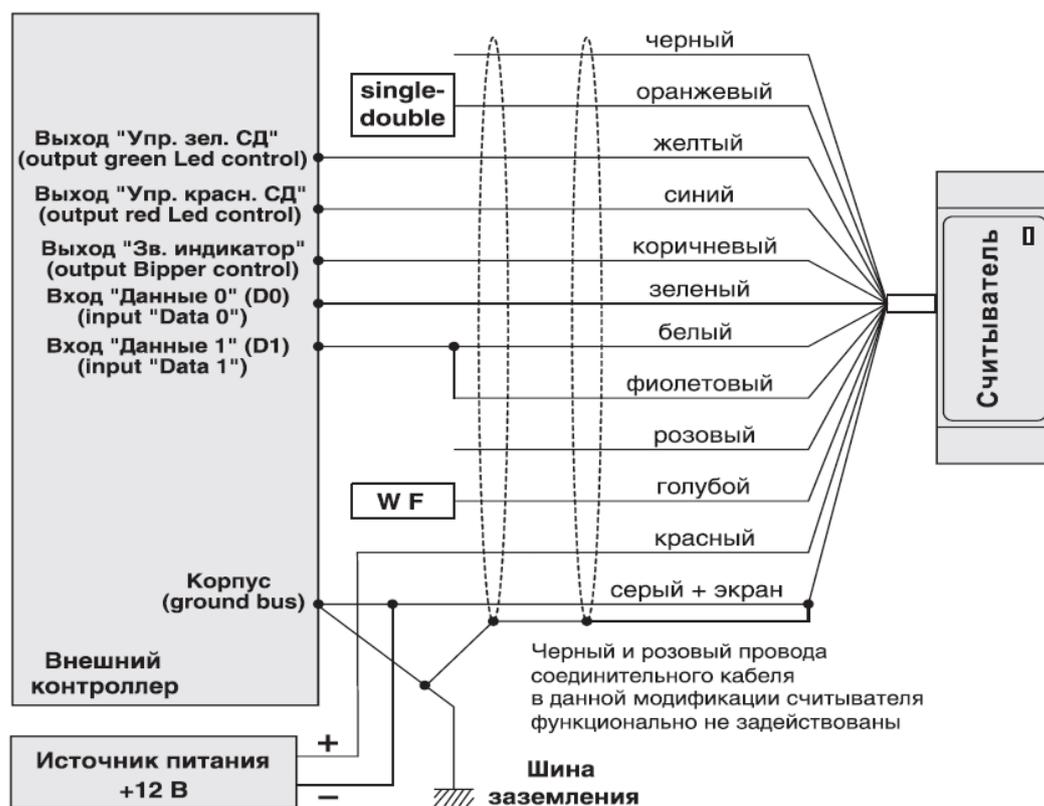
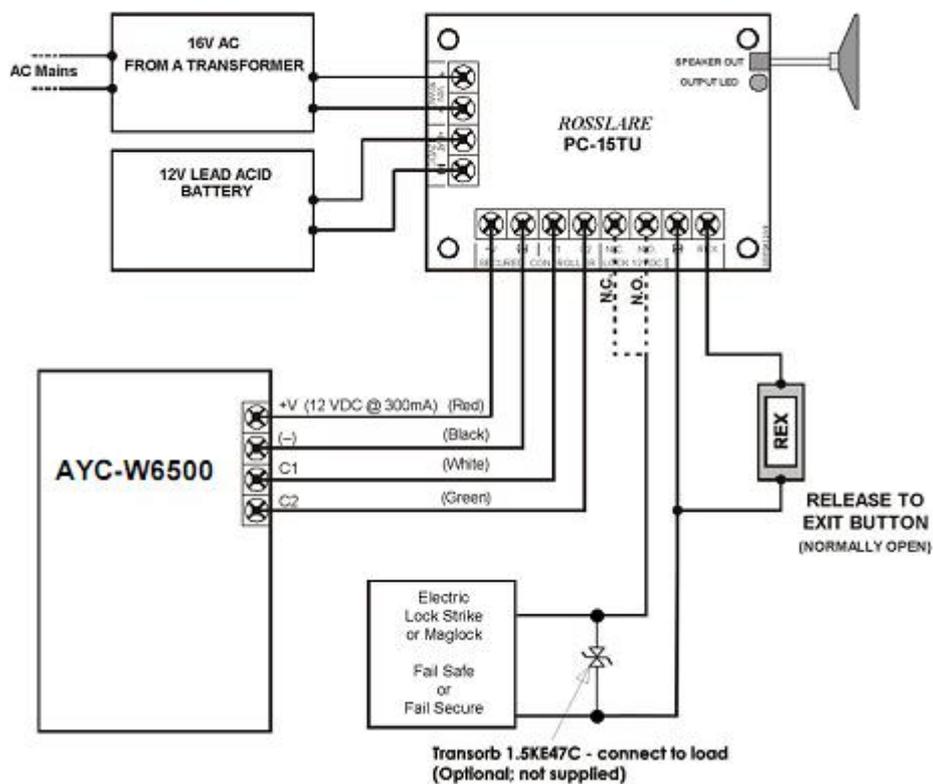


Рис. 1.7. Схема подключения считывателя к контроллеру с использованием интерфейса Wiegand

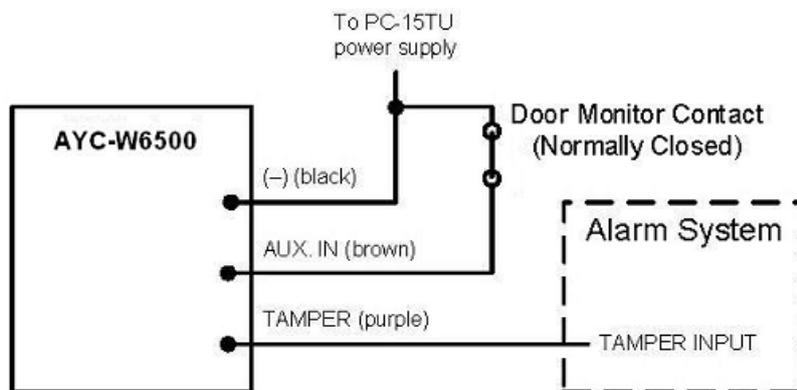
Устройство биометрической идентификации АУС-W6500 производителя Rosslare является интегрированным считывателем и контроллером [8].

Если устройство подключено к специализированным устройствам СКУД АС-C15Т or PS-C15Т, то может работать в качестве контроллера, как показано на рис. 1.8.

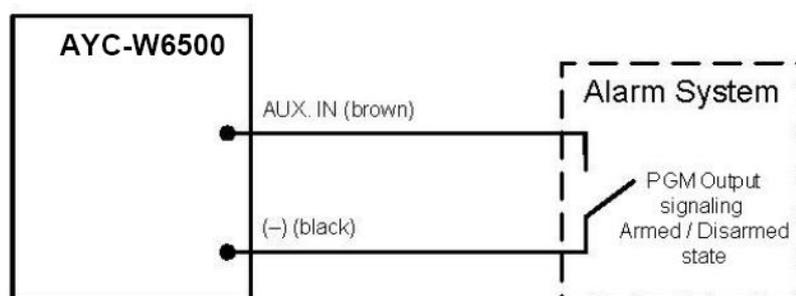
Если устройство подключено к стандартному контроллеру доступа, то работает как считыватель на точку прохода, как показано на рис. 1.9.



a)



б)



в)

Рис. 1.8. Структурная схема подключения устройства, работающего в качестве контроллера, к контроллеру PS-C15TU:

а) общая структура; б) подключение антисаботажного канала;

в) подключение тревожного канала

с нормально разомкнутыми контактами

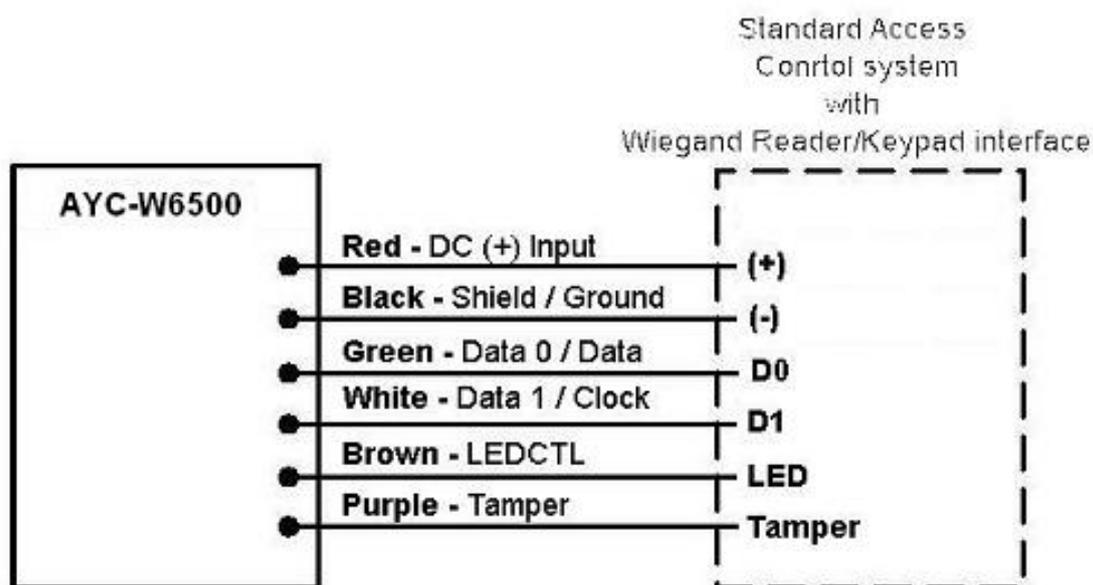


Рис. 1.9. Структурная схема подключения устройства, работающего в качестве считывателя, к стандартному контроллеру системы контроля доступа с интерфейсом Wiegand

Кроме того, устройство может быть подключено по интерфейсу RS-232 к последовательному порту компьютера (см. рис. 1.10).

Когда устройство работает в качестве считывателя, то передача данных о номере карты доступа или PIN-коде, введенном пользователем с клавиатуры, производится только после успешной верификации отпечатка пальца со сканера устройства.

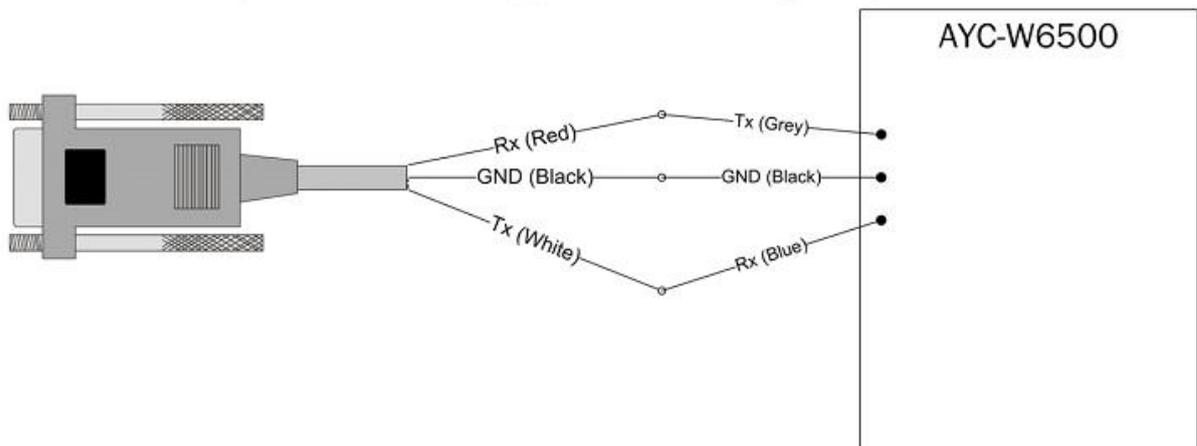


Рис. 1.10. Разводка соединений при подключении устройства по интерфейсу RS-232

Когда устройство работает в качестве контроллера, то открытие двери производится после считывания номера карты доступа или PIN-кода, введенного пользователем с клавиатуры, подтвержденных успешной верификации отпечатка пальца со сканера устройства.

Емкость устройства рассчитана на 500 пользователей и 1000 отпечатков пальцев и поддерживает ввод данных о номере карты доступа, персонального идентификационного номера, введенного пользователем с клавиатуры (PIN-кода), и данных отпечатка пальца.

Длина PIN-кода может быть установлена фиксированной в 4, 5, 6 цифр или переменной от 4 до 8 цифр.

Тактико-технические характеристики приведены в табл. 1.3.

Тактико-технические характеристики устройства

Параметр	Значение
Напряжение питания	+10 – +16 В (обеспечивается контроллерами PS-C15T или AC-C15TU, когда устройство работает как контроллер)
Входной ток	140 mA при 12 В
Выходной ток	330 mA при 16 В
Тип выходных контактов	открытый коллектор антисаботажного выхода тревоги
Тип входных контактов	сухие контакты, нормально открытые 0–5 В
Длина кабеля	до 150 м
Режимы работы	- нормальный: PIN-код или карта доступа + отпечаток пальца; - повышенной безопасности: PIN-код + карта доступа + отпечаток пальца
Количество отпечатков пальцев	до 1000
Количество пользователей	500
Время верификации	менее 1,5 сек
Мак дальность считывания карт	до 7,5 см
Карта доступа	Proximity card, модуляция ASK, 125 KHz, совместимость EM cards, формат передачи данных 26-bit Wiegand или Clock & Data
Клавиатура	3×4 =12 клавиш, формат передачи данных — программируемые форматы PIN-кода
Индикатор	трехцветный светодиодный

Параметр	Значение
Выходной формат данных	Wiegand 26 Bits, RS-232
Частота возникновения ошибки I рода (события «ложный отказ»)	0,01
Частота возникновения ошибки II рода (события «ложный допуск»)	0,002
Коэффициент равной вероятности ошибок I и II рода	0,001

1.2.2. Программное обеспечение СКУД

1.2.2.1. Порядок работы с системой при конфигурировании с помощью программного обеспечения, установленного на персональном компьютере

Базовый комплект поставки системы состоит из ПО сервера аппаратуры, соответствующего типу приобретенных контроллеров, и базового пакета, в который входят следующие модули [6, 7]:

- Консоль администратора БД;
- Консоль управления со следующими разделами:
 - Конфигуратор;
 - Справочники доступа;
 - Персонал (с модулем «Оформление пропусков»);
 - Отчеты;
 - Доступ на объекты;
 - Мониторинг;
- Сервер системы;
- Сервер управления данными;
- Сервер БД.

В качестве сервера БД используется SQL-сервер FireBird.

Можно организовать работу системы, установив все ПО на один компьютер или распределив модули по разным хостам.

Кроме базового комплекта ПО, обеспечивающего работу системы в целом, существуют или разрабатываются дополнительные компоненты, расширяющие основные функции системы. Они включают в себя следующие модули: Учет рабочего времени; Видеоидентификация; Мониторинг с мнемосхемами; Интеграция с системой видеонаблюдения; Интеграция с охранно-пожарной сигнализацией; Планировщик задач; Мастер отчетов.

ПО поддерживает следующие функции:

- управление подсистемами контроллеров 600 серии (до 64 на один сервер аппаратуры) и 12 000 серии (до 255 на один сервер аппаратуры), а также сбор информации с них, при этом на одном компьютере не может быть двух серверов аппаратуры одинаковой серии;

- проведение автоконфигурации системы;

- задание различных прав доступа пользователям ПО системы с помощью паролей;

- оформление пропусков;

- задание индивидуальных графиков доступа сотрудников в помещения;

- ведение базы данных персонала;

- подключение системы видеонаблюдения;

- подключение системы охранно-пожарной сигнализации;

- формирование отчетов: о рабочем времени сотрудников;

- мониторинг и управление аппаратурой с рабочего места оператора;

- защита от передачи карт доступа при проходе через точку доступа;

- управление базами данных и контроль за их сохранностью.

Конфигурирование системы производится с рабочего места с помощью ПО, установленного на компьютере, как более наглядно демонстрирующее возможности системы, хотя те же операции можно производить и в автономном режиме с клавиатуры биометрического считывателя, но без языковой и визуальной индикации производимых событий для учебных целей такие операции затруднены.

Настройка СКУД производится в три этапа:

1. С помощью настольного бесконтактного считывателя пластиковых карт и ПО PERCo-S-600 производится заполнение базы пользователей кодами карт.

2. С помощью преобразователя интерфейсов, контроллера PERCo-SC-600 и ПО PERCo-S-600 производится заполнение базы пользователей правами управления устройствами.

3. С помощью биометрического считывателя и ПО BioTrax производится заполнение базы биометрических данных пользователей с использованием данных кодов карт пользователей, полученных при выполнении п. 1.

После выполнения конфигурирования с помощью ПО компьютера СКУД может работать как в автономном режиме, так и под управлением компьютера.

Порядок операций при конфигурировании СКУД согласно вышеприведенным трем этапам следующий:

1) подключить интерфейсный кабель RS-232 настольного считывателя карт к СОМ- порту компьютера;

2) включить питание настольного считывателя;

3) включить питание компьютера;

4) запустить ПО Perco;

5) ввести пользователей системы и занести коды карт пользователей в базу, используя настольный считыватель карт:

- интерфейс программы Perco для введения пользователей приведен на рис. 1.11, на котором в дереве команд для выделенного раздела «Персонал», выбрав вкладку «Новый сотрудник» можно ввести личные данные пользователя системы, включая фотографию;

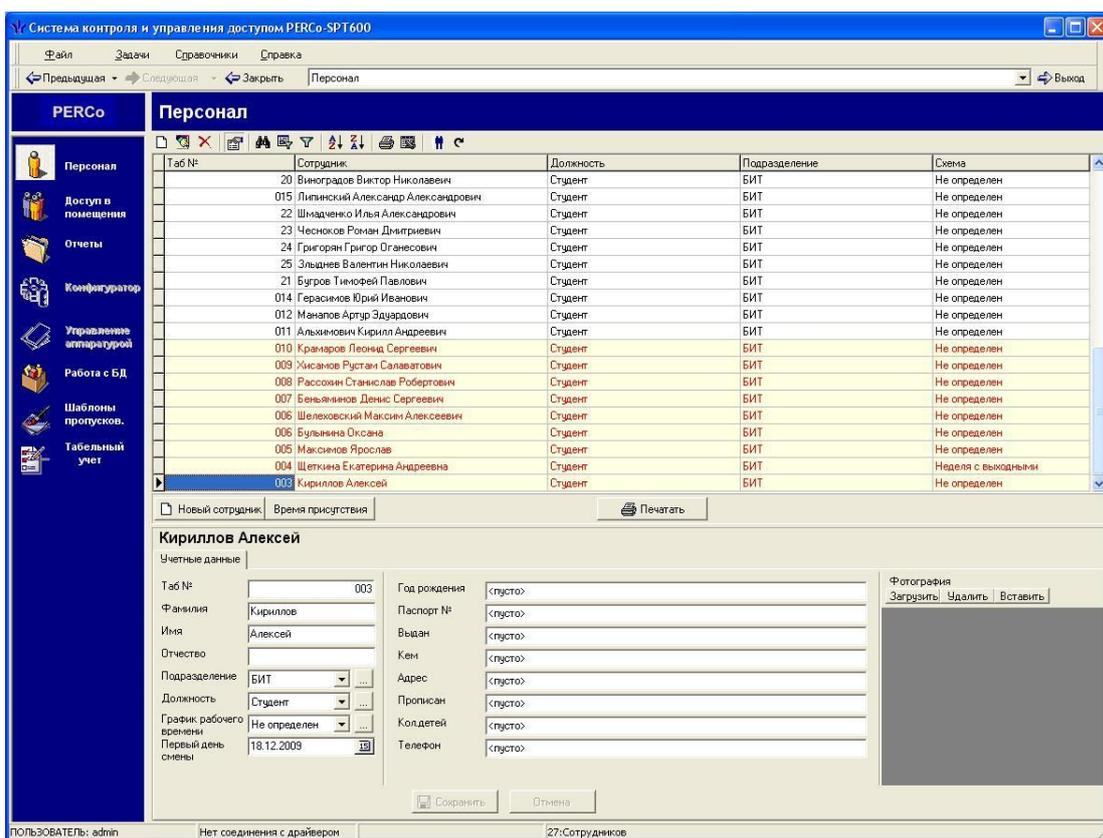


Рис. 1.11. Ввод личных данных пользователей СКУД

- для организации доступа в помещения в дереве команд используется раздел «Доступ в помещения», здесь для выбранного сотрудника на вкладке «Пропуска» выбираем кнопку «Выдать» и в момент, когда появится новое окно выдачи пропуска, нажать в нем кнопку «Старт» и поднести карту доступа к настольному считывателю карт — результатом будет занесение серии и номера карты, что необходимо подтвердить соответствующей кнопкой «ОК» (см. рис. 1.12);

- далее для выбранного сотрудника на вкладке «Доступ» с помощью кнопки «Предоставить» производится предоставление доступа к устройствам управления (замкам) дверей в СКУД, как показано на рис. 1.13.

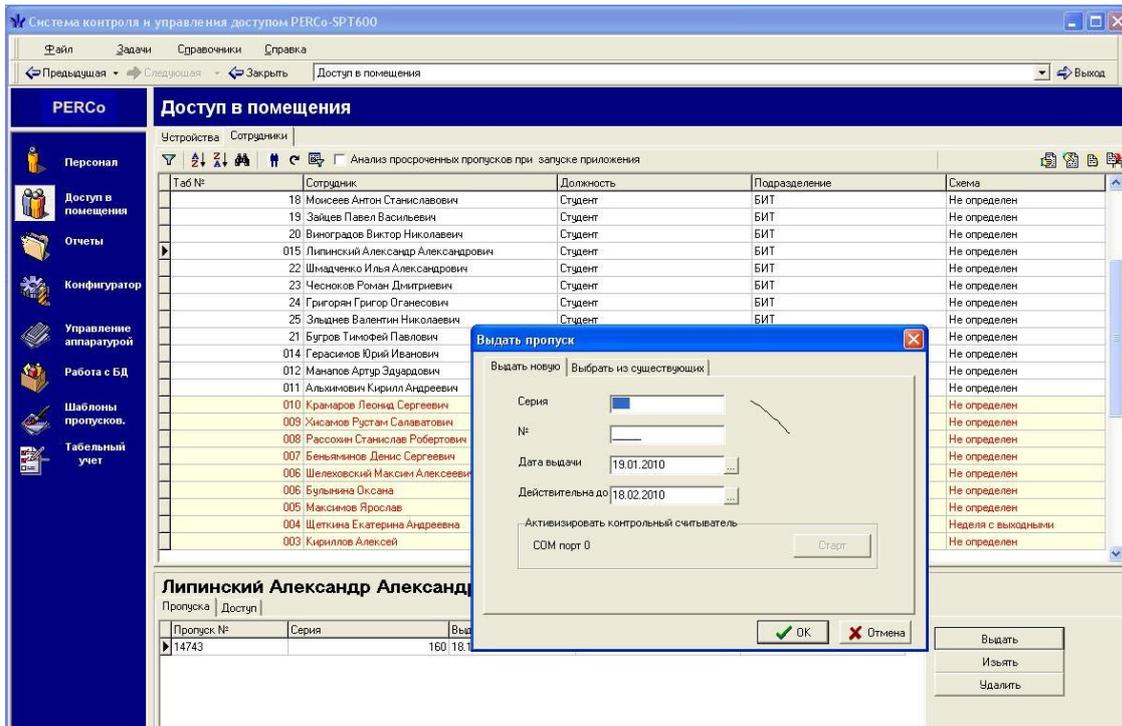


Рис. 1.12. Считывание серии и номера карты для занесения в базу данных сотрудников

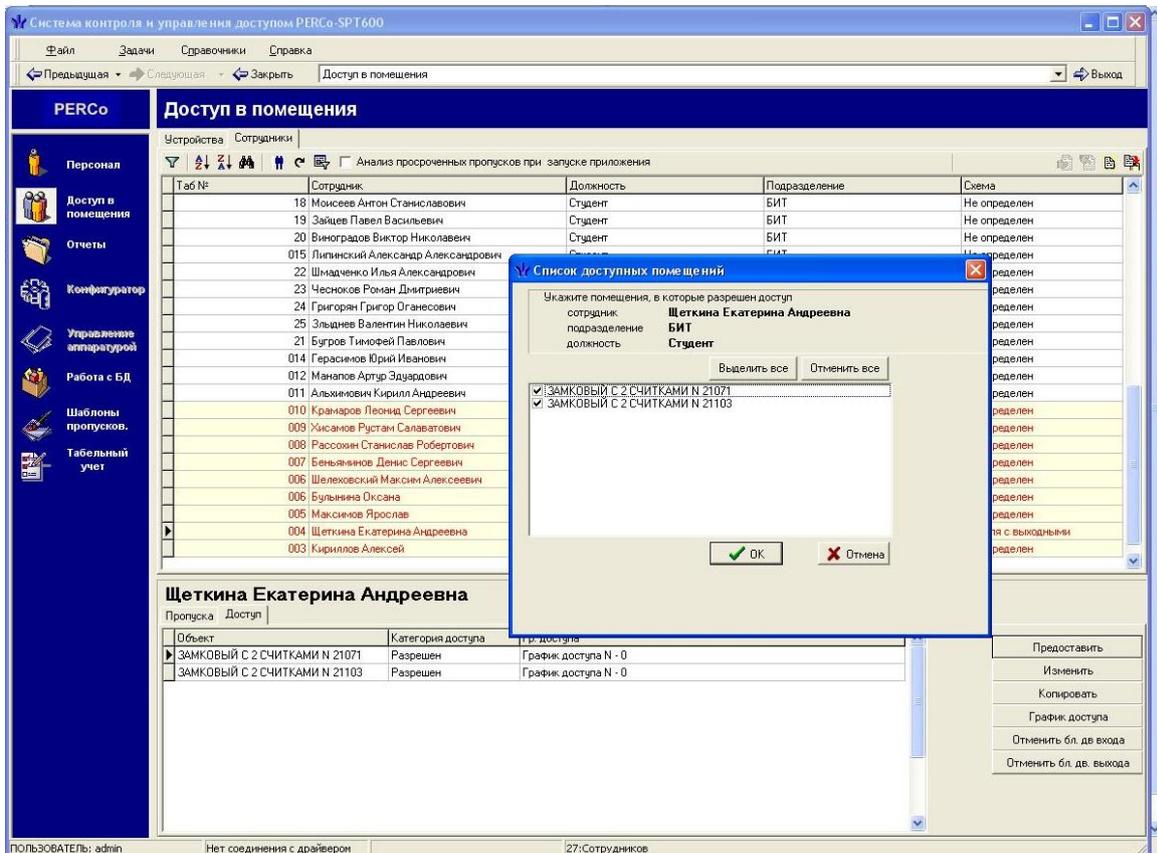


Рис. 1.13. Предоставление доступа выбранному пользователю к доступным помещениям

- категория доступа в помещение может быть изменена с помощью кнопки «Изменить», как показано на рис. 1.14;

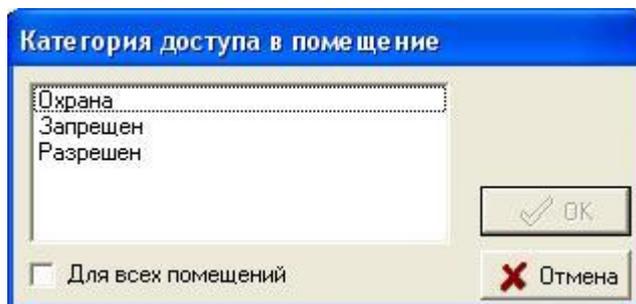
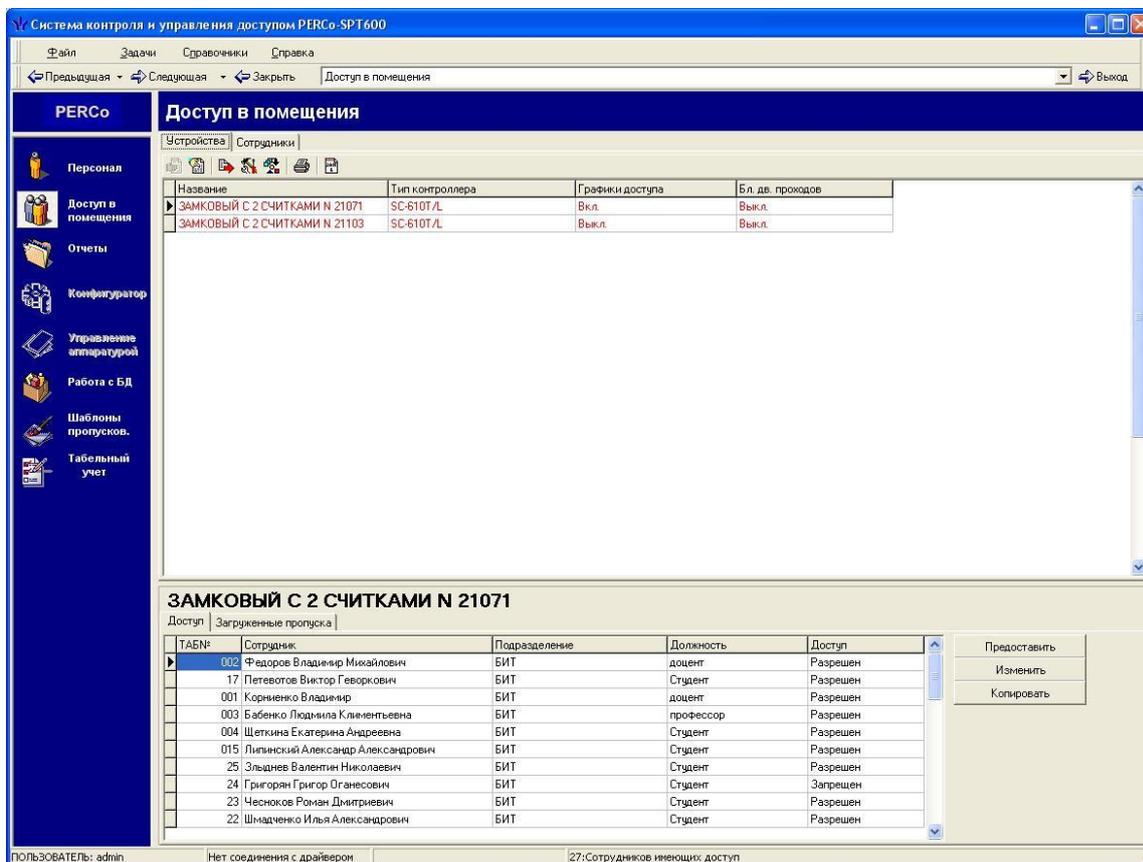
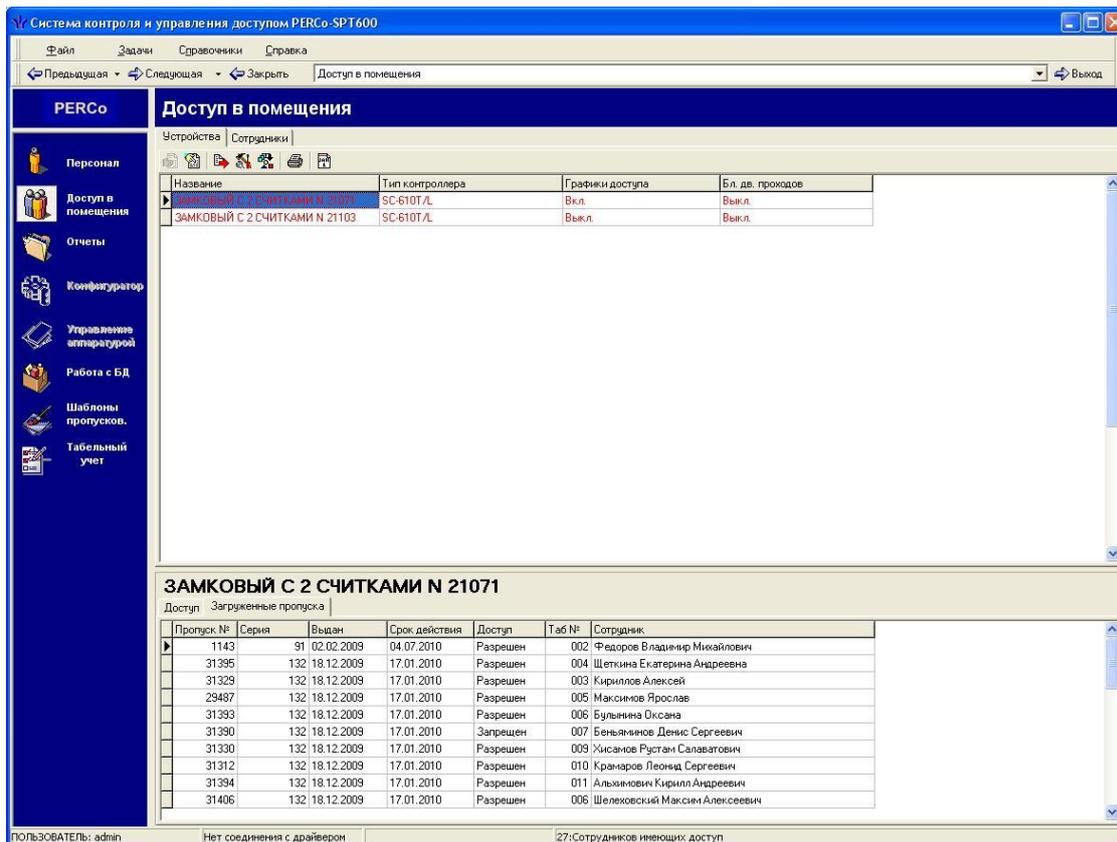


Рис. 1.14. Изменение категории доступа выбранного пользователя в помещения

- на вкладке «Устройства» раздела доступа в помещение можно для выбранного устройства управления посмотреть доступ и загруженные пропуска, а также предоставить или изменить доступ, как было сделано ранее, что показано на рис. 1.15.



а)



б)

Рис. 1.15. Доступ (а) и загруженные пропуска (б) для выбранного устройства управления

б) закрыть приложение и выключить компьютер и блок питания настольного считывателя;

7) для занесения кодов карт пользователей с помощью дверного считывателя карт необходимо проделать подп. 1–8, только при подключении к компьютеру соответствующего интерфейсного кабеля RS-232 от преобразователя интерфейса RS-485/RS-232;

8) выключить компьютер;

9) подключить интерфейсный кабель RS-232 контроллера PERCo-SC-600 со считывателем карт, идущий от преобразователя интерфейсов, к COM-порту компьютера;

10) включить питание настольного преобразователя интерфейсов RS-485/RS-232;

11) включить питание компьютера;

12) запустить ПО Perco;

13) настроить управление устройствами (замками) для пользователей системы, как показано на рис. 1.13–1.15, настроить график доступа и временные интервалы доступа для каждого пользователя (см. рис. 1.16 и 1.17), но если записи в списке пользователей выделены красным цветом, то это означает, что для конкретного сотрудника в категории доступа не разрешен доступ во все помещения, а при предоставлении доступа во все помещения выделение красным цветом снимается, что показано на рис. 1.18, и только после проведенных операций загрузить данные с компьютера в контроллер (см. рис. 1.16);

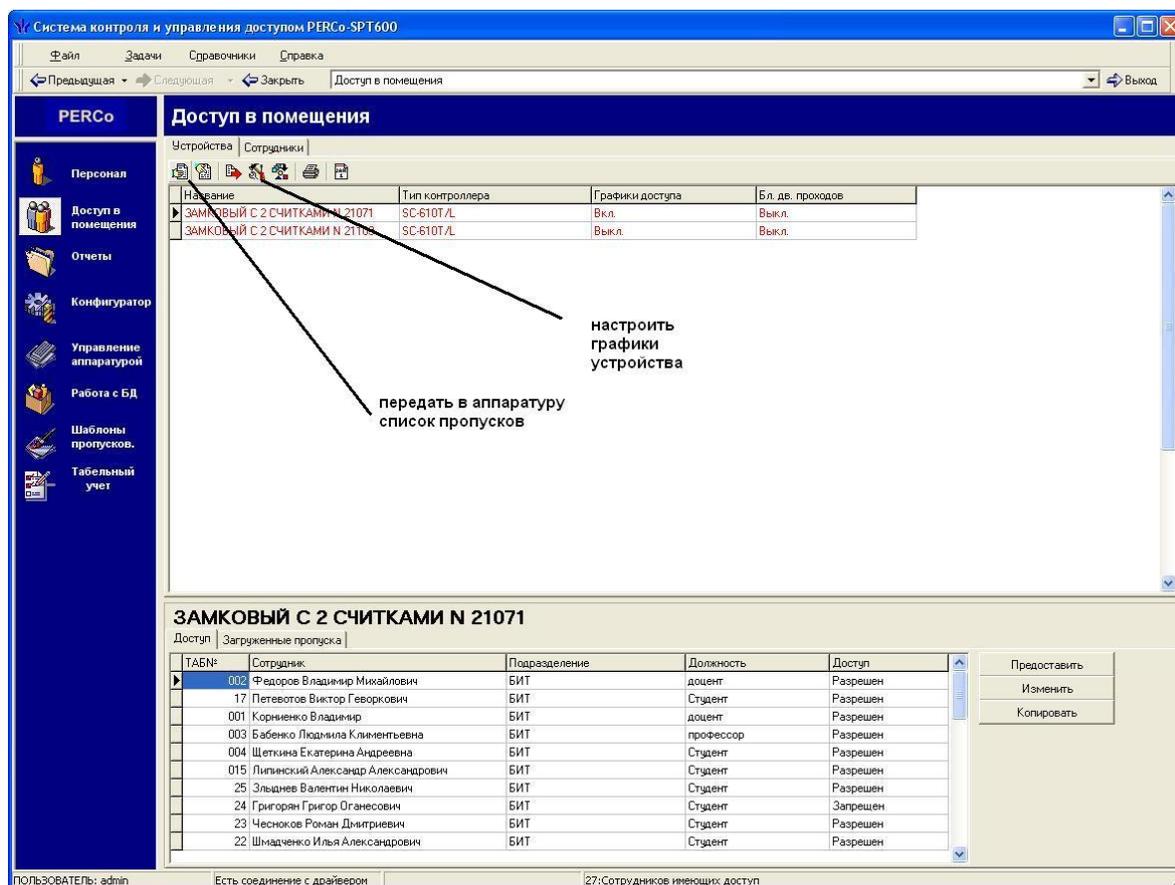


Рис. 1.16. Вызов настройки графиков доступа для устройств управления электромагнитными замками и загрузка кодов карт пользователей в контроллер

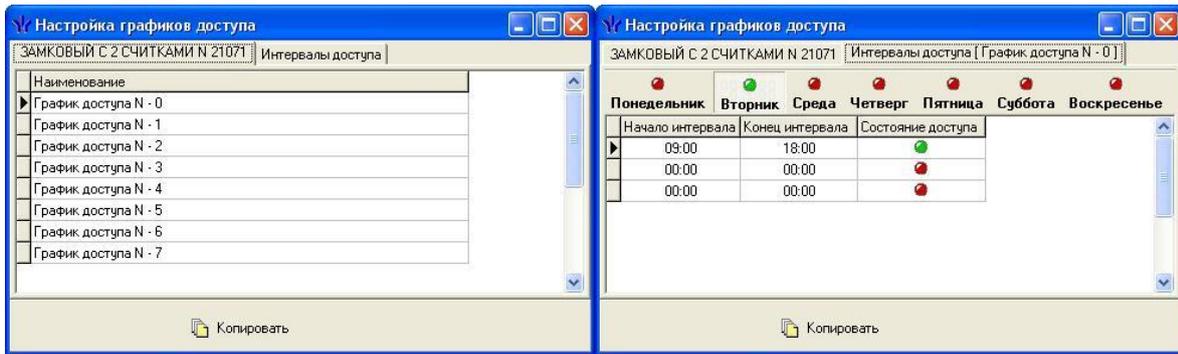
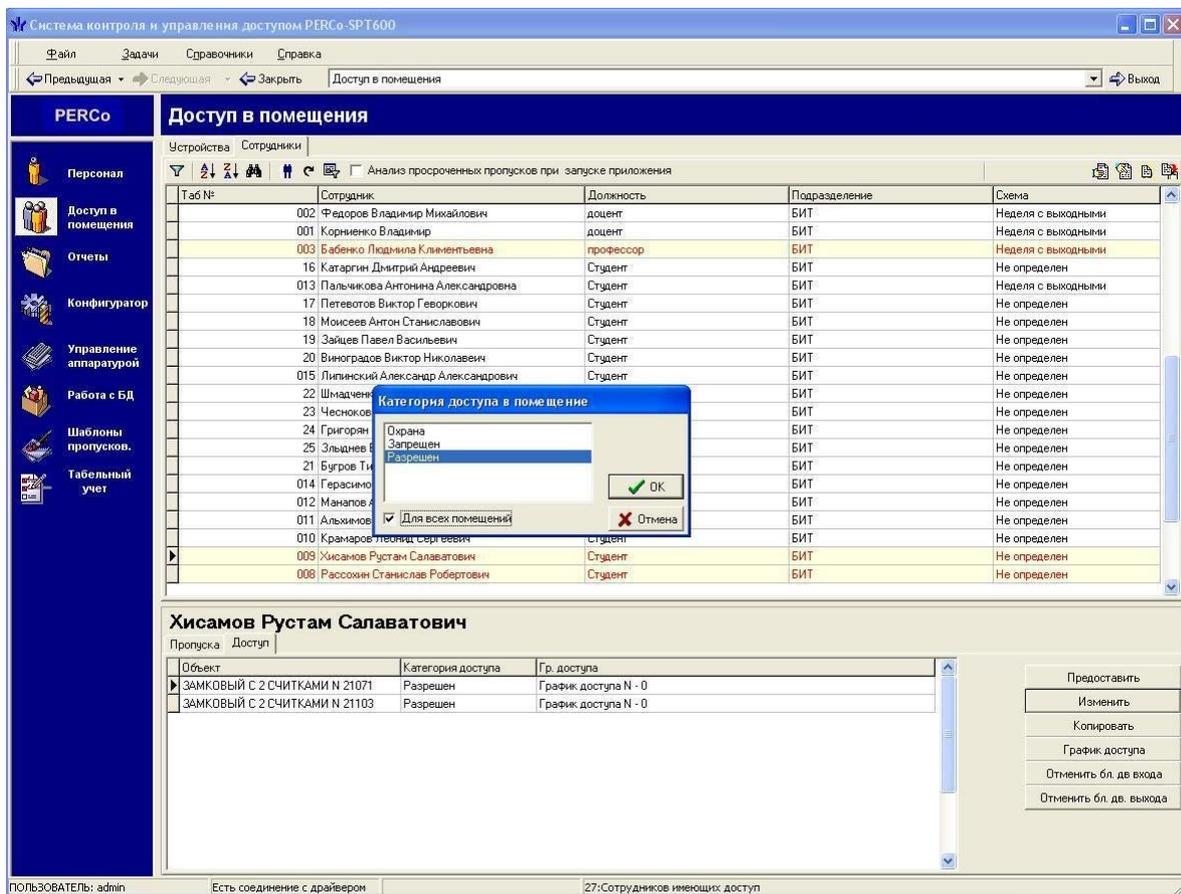
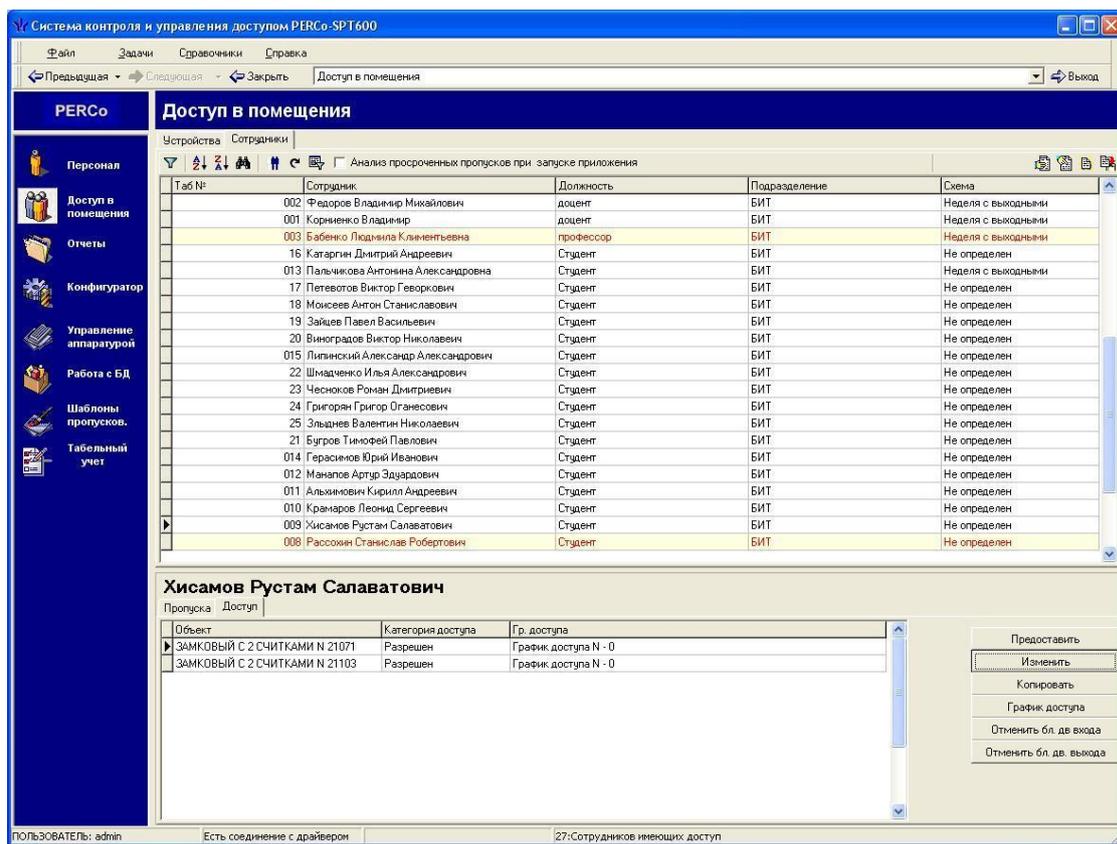


Рис. 1.17. Настройка графиков доступа (а)
и временных интервалов для графиков доступа (б)



а)



б)

Рис. 1.18. Снятие выделения красным цветом в случае предоставления доступа во все помещения:

а) до разрешения доступа; б) после предоставления доступа

14) в дереве команд, используя раздел «Конфигуратор» (см. рис. 1.19), можно настроить реакции оборудования при открывании дверей: подачу звукового сигнала, тип пульта дистанционного управления (при выходе из помещения, например, используется кнопка выхода), время удержания замка в открытом состоянии, включить графики доступа, включить блокировку дверного прохода, обеспечив защиту от передачи карт;

15) в дереве команд, используя раздел «Управление аппаратурой», (см. рис. 1.20) выбрать режим управления, а также включить запрет использования карты для выбранного пользователя СКУД в случае утери карты или при увольнении сотрудника (для восстановления кода карты в системе потребуется удалить пользователя из системы, а затем вновь ввести для него данные);

16) в дереве команд, используя раздел «Работа с БД», (см. рис. 1.21) выполнить администрирование, поддержание целостности базы данных, подключение оборудования к портам компьютера;

17) выключить компьютер.

Перед занесением биометрических данных пользователей с помощью считывателя отпечатков пальцев необходимо предварительное занесение пользователей и кодов их карт, согласно подп. 1–6;

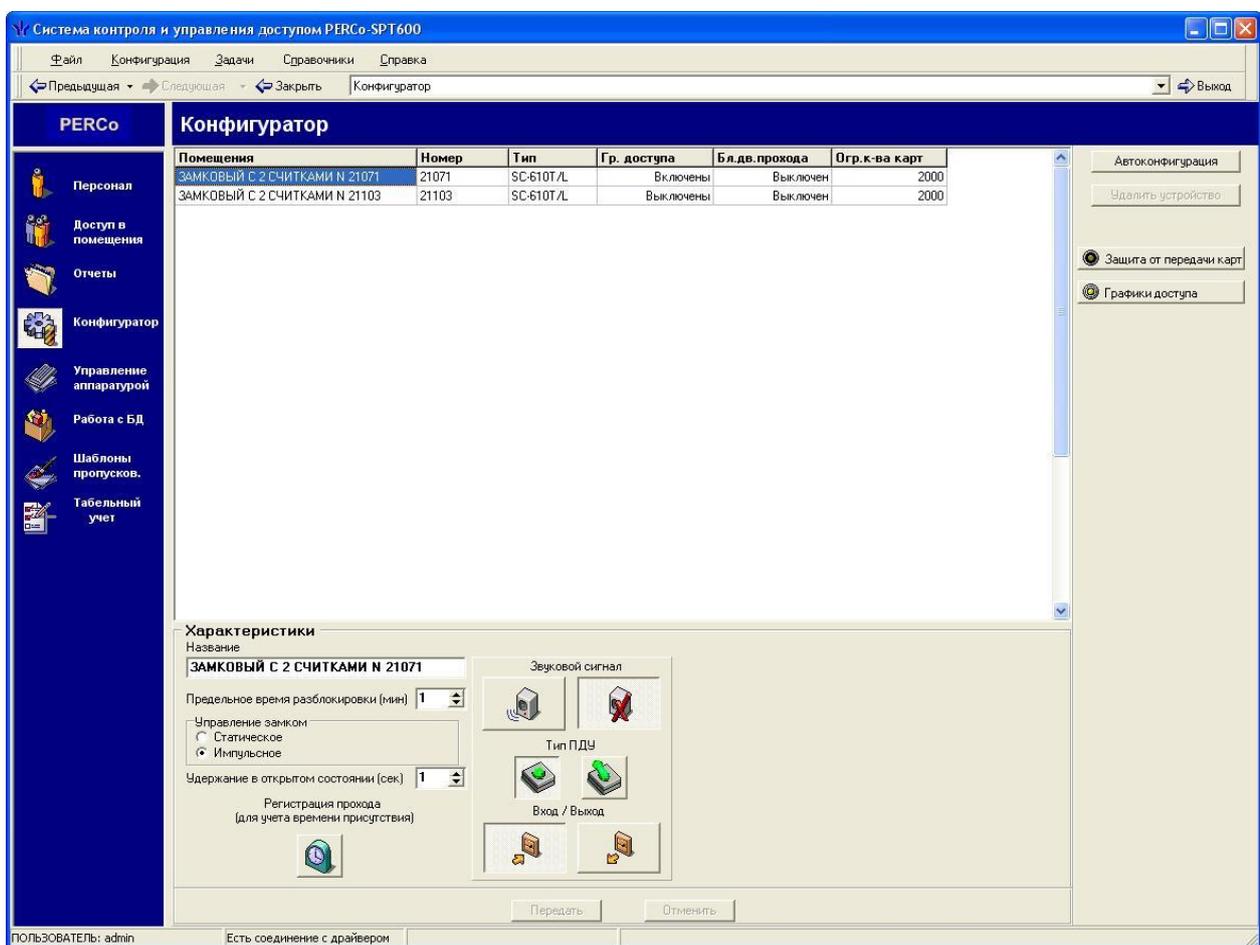


Рис. 1.19. Конфигурирование замков

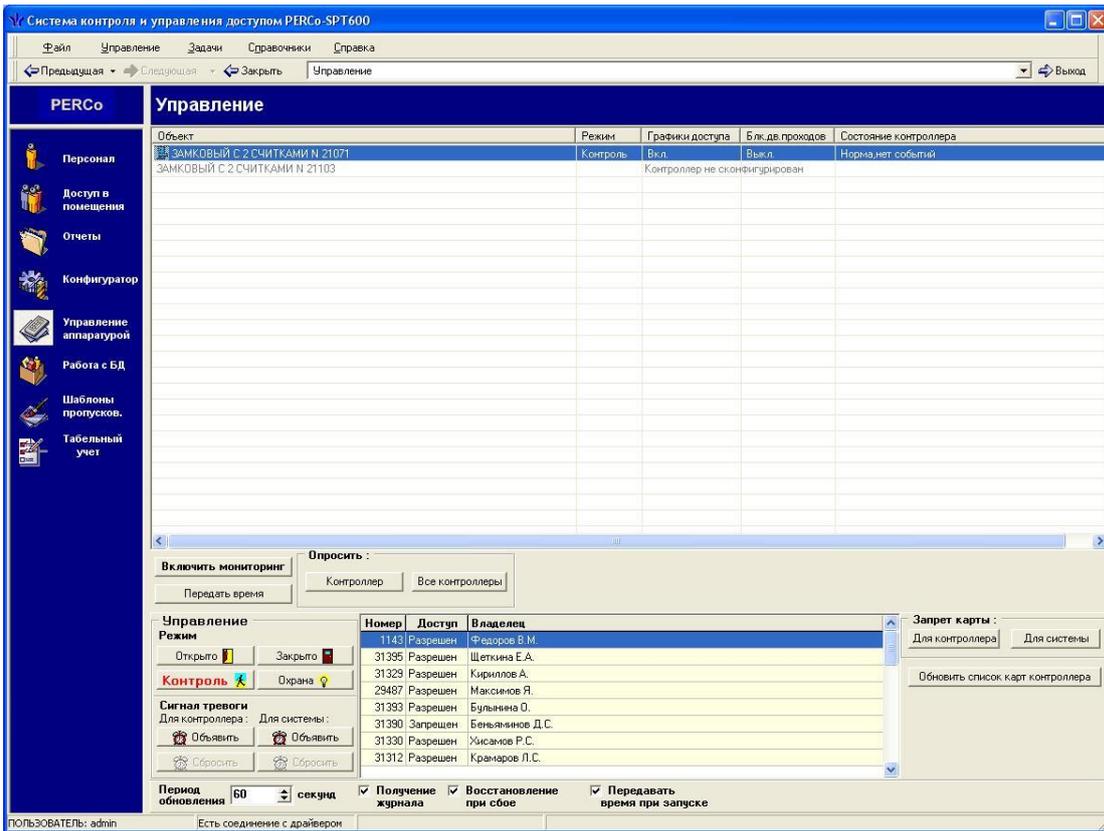


Рис. 1.20. Управление аппаратурой

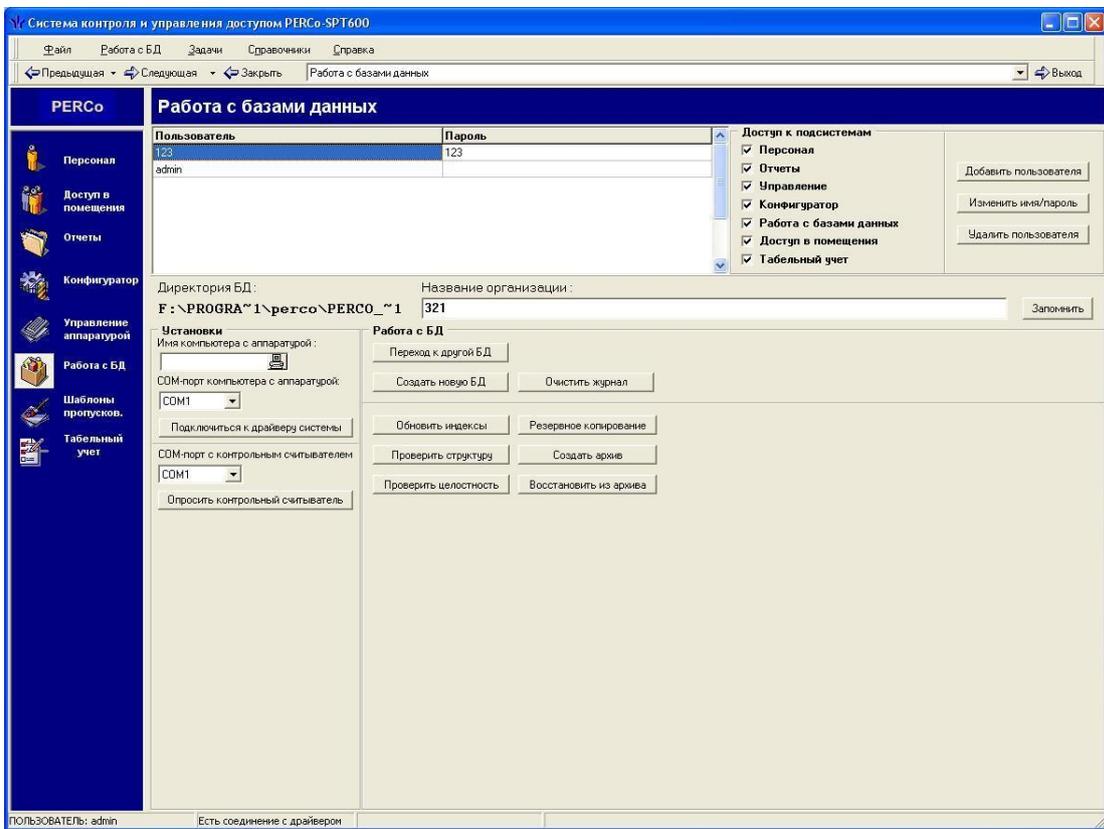


Рис. 1.21. Администрирование базы данных

18) подключить интерфейсный кабель RS-232 биометрического считывателя, идущий от преобразователя интерфейсов, к порту компьютера;

19) включить питание контроллера Perso и компьютера;

20) запустить ПО BioTrax, при этом аппаратное конфигурирование считывателя/контроллера BioTrax проведено заранее [8], как показано на рис. 1.9, поэтому для начала необходимо ввести пользователей и коды их карт, выделив в дереве команд раздел Card, как показано на рис. 1.22;

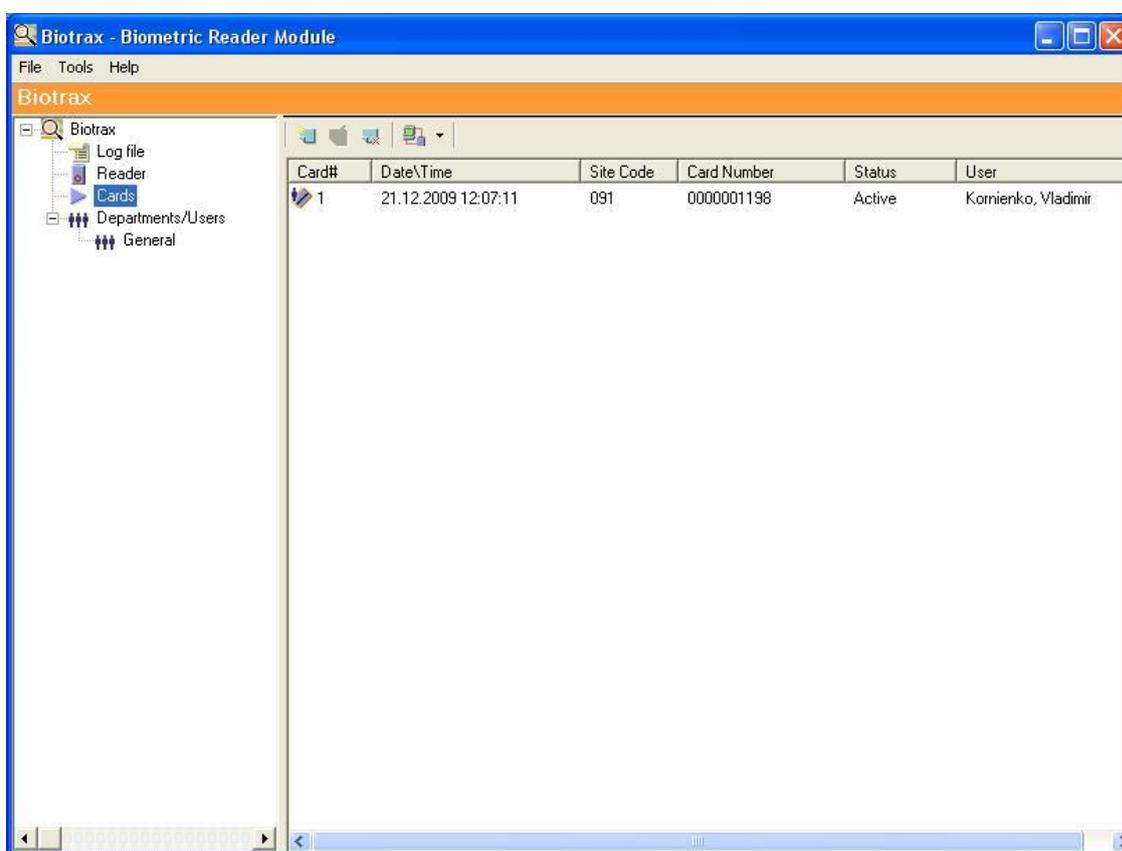


Рис. 1.22. Использование дерева команд для настройки ПО BioTrax

21) на панели инструментов нажать кнопку добавления новой карты и в появившемся окне ввести в поле Card Quantity число добавляемых карт, в поле Start from — 6-ти значный номер карты, поддерживающей интерфейс Wiegand, а в поле Site code — 2-х значное значение серии карты, после чего нажать Add, как показано на рис. 1.23;

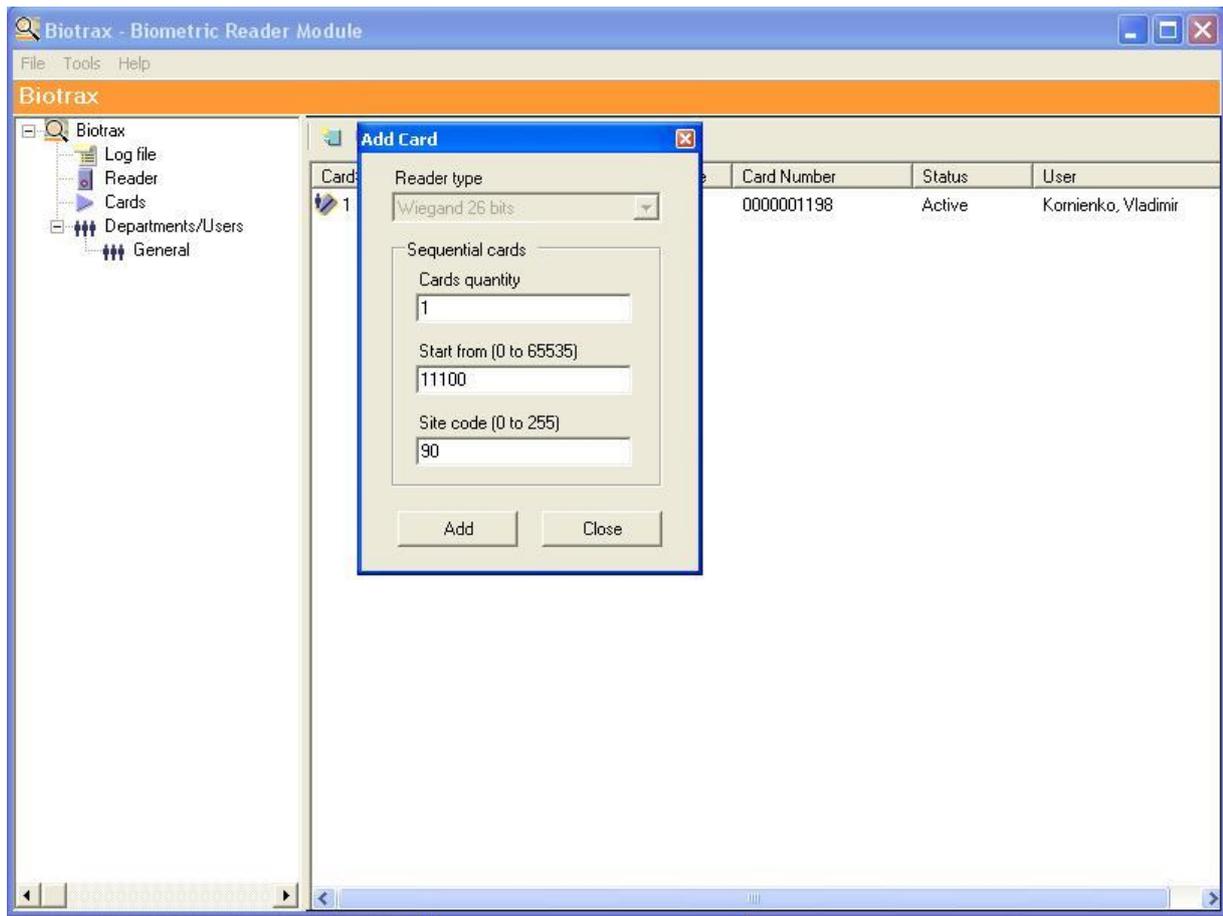


Рис. 1.23. Добавление карт пользователей

22) добавить пользователей системы, для чего в дереве команд раскрыть раздел Department/Users и выделить подраздел General, как показано на рис. 1.24;

23) на панели инструментов нажать кнопку добавления нового пользователя и в появившемся окне на вкладке General ввести табельный номер пользователя, Имя, Фамилию, фотографию, как показано на рис. 1.25;

24) ввод PIN-кода доступа с клавиатуры считывателя, кода карты производится в том же окне ввода свойств пользователей на вкладке Codes, где для начала производится добавление кода карты пользователя, нажатием кнопки Add from list, как показано на рис. 1.26, затем осуществляется ввод 4-х значного PIN-кода, который нужно будет набирать для доступа в помещение с клавиатуры считывателя;

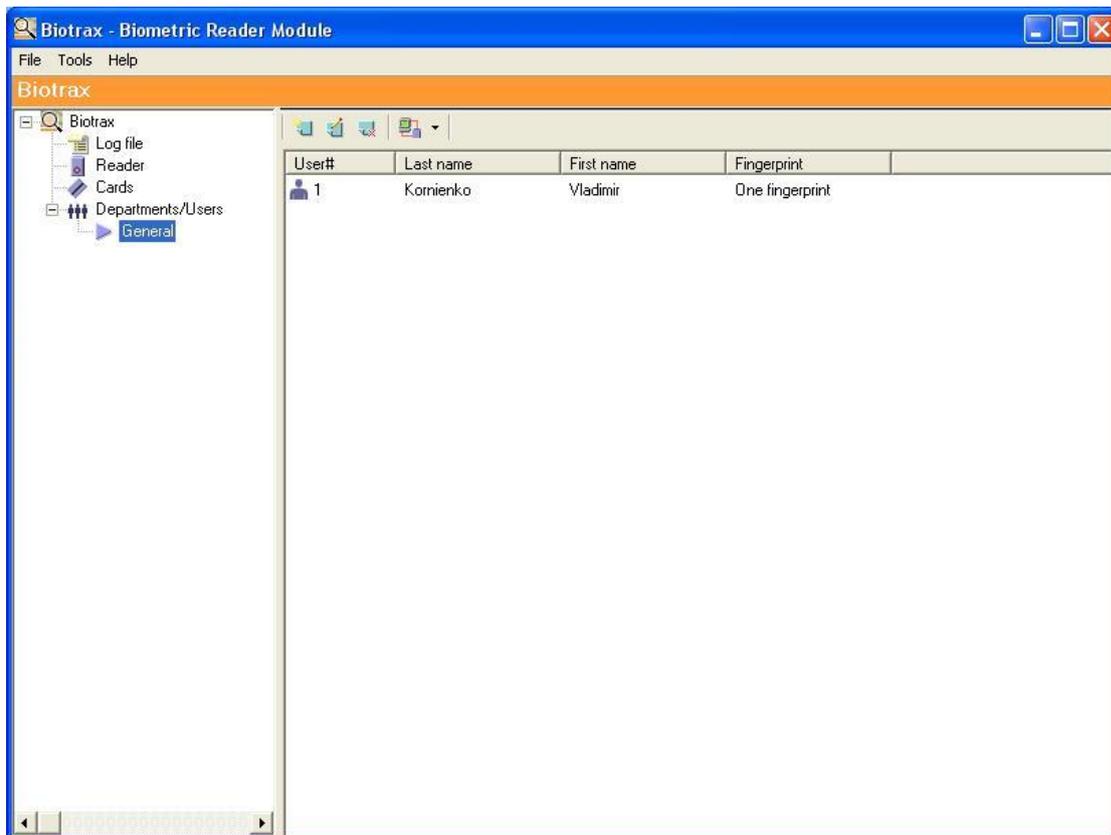


Рис. 24. Вход в режим добавления пользователей

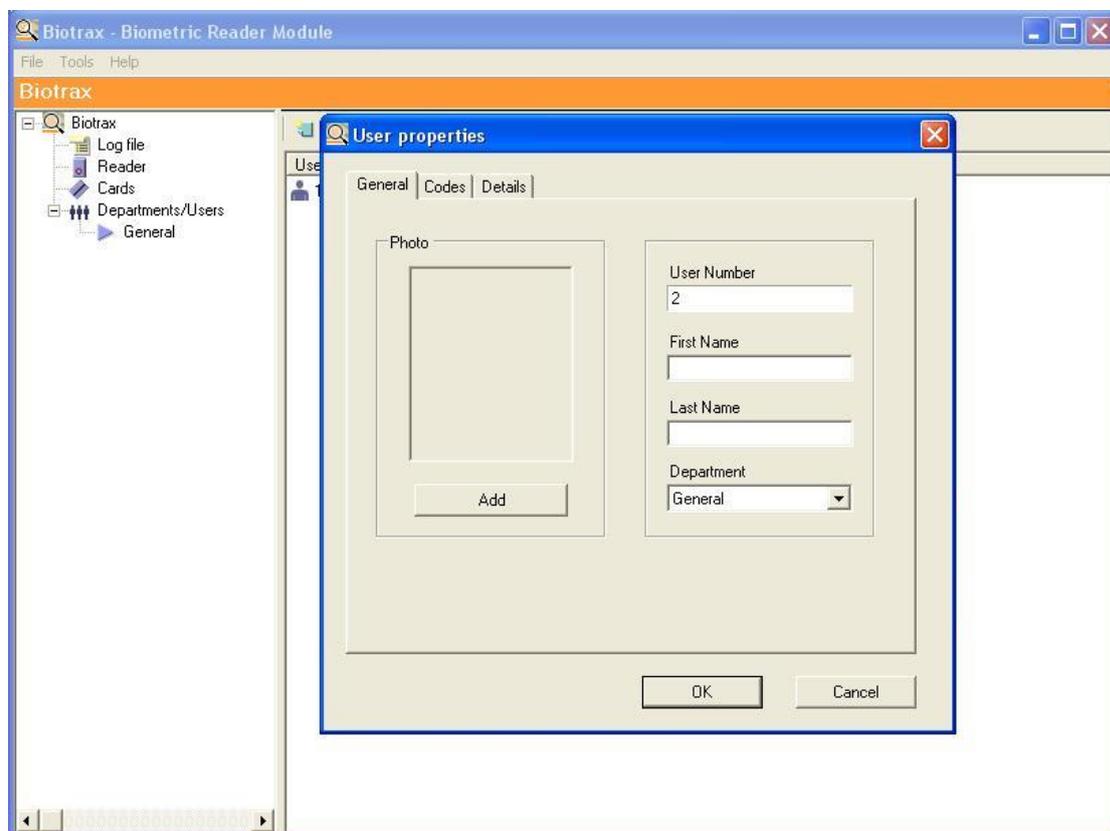


Рис. 25. Добавление информации о пользователе СКУД

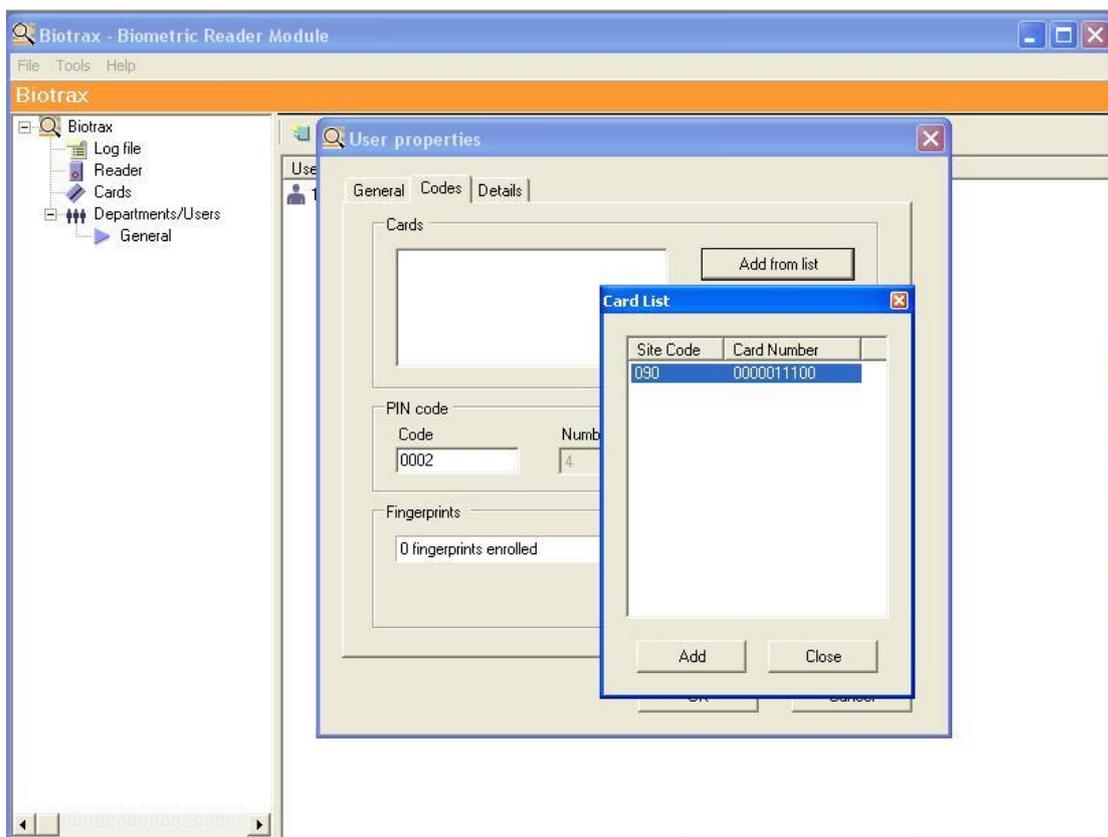


Рис. 1.26. Добавление кода карты пользователя

25) для добавление отпечатков пальцев в том же окне ввода свойств пользователей на вкладке Codes необходимо в панели Fingerprints нажать кнопку Add, после чего пользователь, для которого производится заполнение свойств доступа, по приглашению Place your finger, как показано на рис. 1.27, прикладывает палец к сканеру биометрического считывателя, расположенного н стене у входа в помещение;

26) после однократного сканирования отпечатка система произведет запрос повторного ввода отпечатка по приглашению Place your finger again, как показано на рис. 1.28;

27) если ввод произведен успешно, то сообщение покажет, что отпечаток введен 1 fingerppints enrolled, как показано на рис. 1.29;

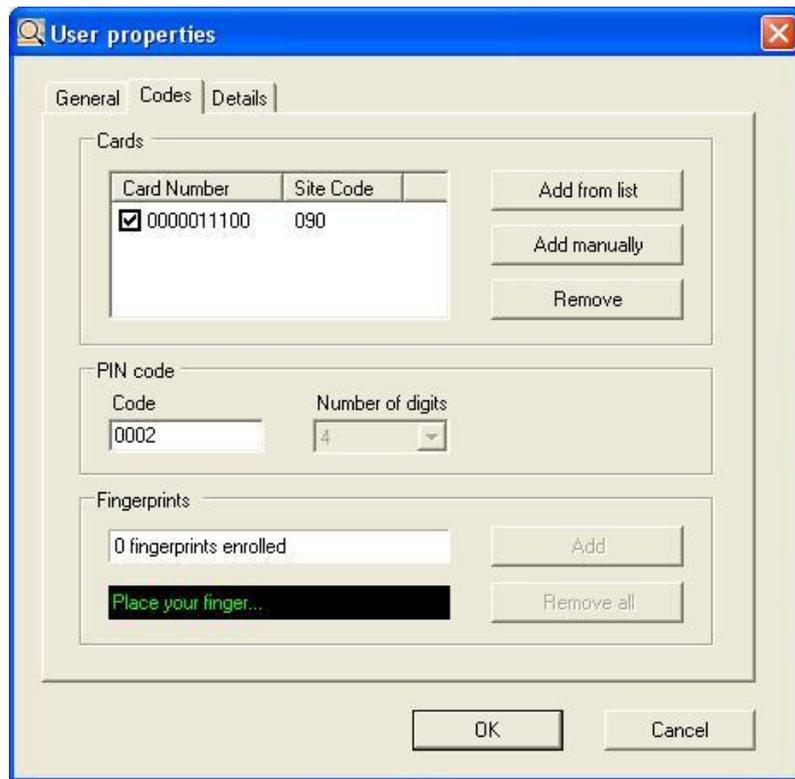


Рис. 1.27. Приглашение к вводу отпечатка пальца пользователя СКУД

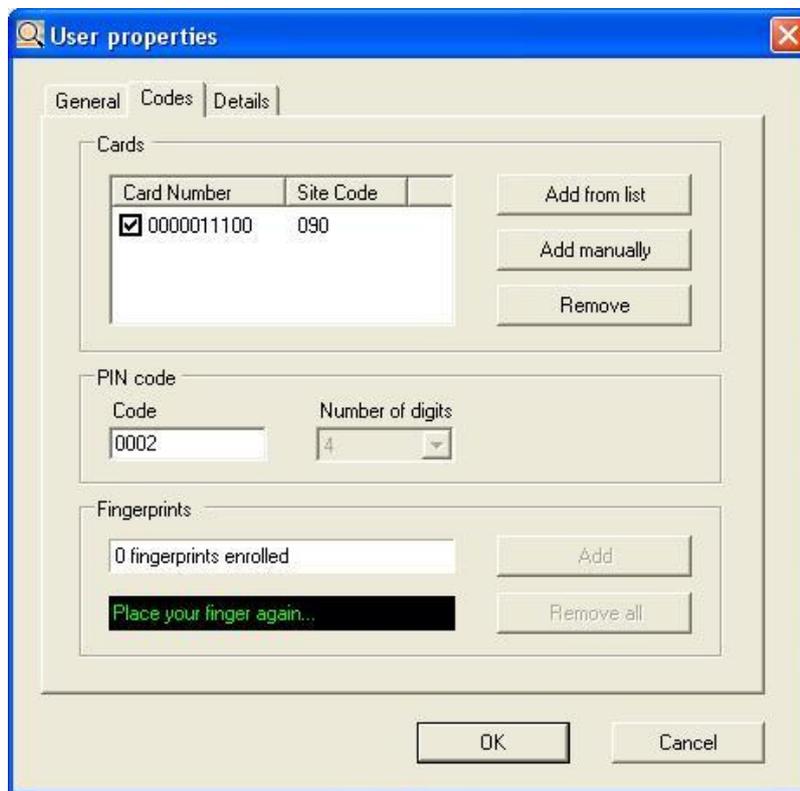


Рис. 28. Приглашение к повторному сканированию отпечатка пальца

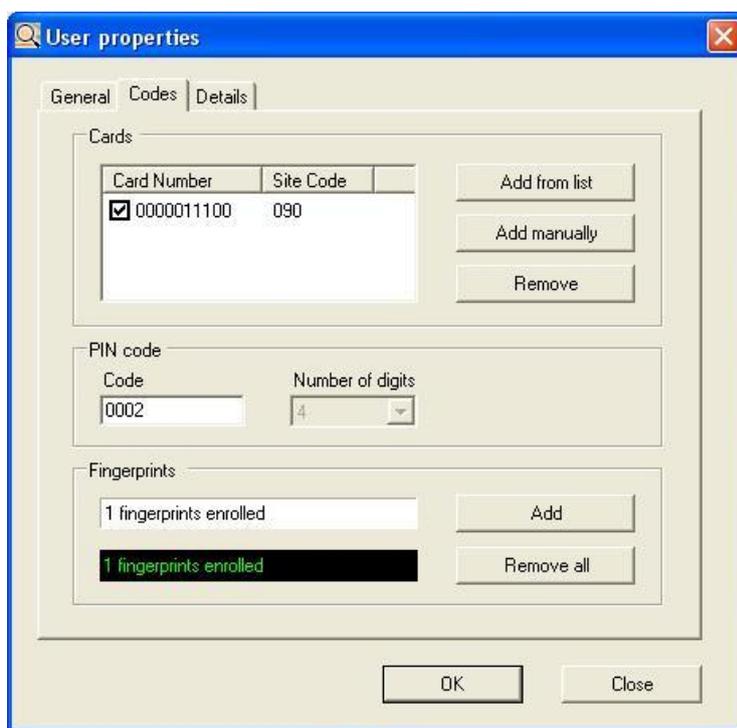


Рис. 29. Успешный ввод отпечатка пальца

28) пользователи системы с введенными кодами карт доступа, PIN-кодами и отпечатками пальцев отображаются в окне подраздела General, как показано на рис. 1.30;

29) для загрузки данных с компьютера в контроллер BioTrax необходимо выполнить команду Download с помощью нажатия 4-й кнопки на панели инструментов;

30) для загрузки данных с BioTraks в компьютер можно выполнить команду Upload в случае, если все настройки проводились непосредственно с клавиатуры BioTrax и были занесены в память контроллера;

31) после занесения пользователей в базу компьютера и память контроллеров можно отключить преобразователь интерфейса от компьютера и работать со СКУД в автономном режиме, используя для доступа в помещение карты доступа, коды доступа и биометрические данные отпечатков пальцев, а для выхода из помещения — кнопку выхода.

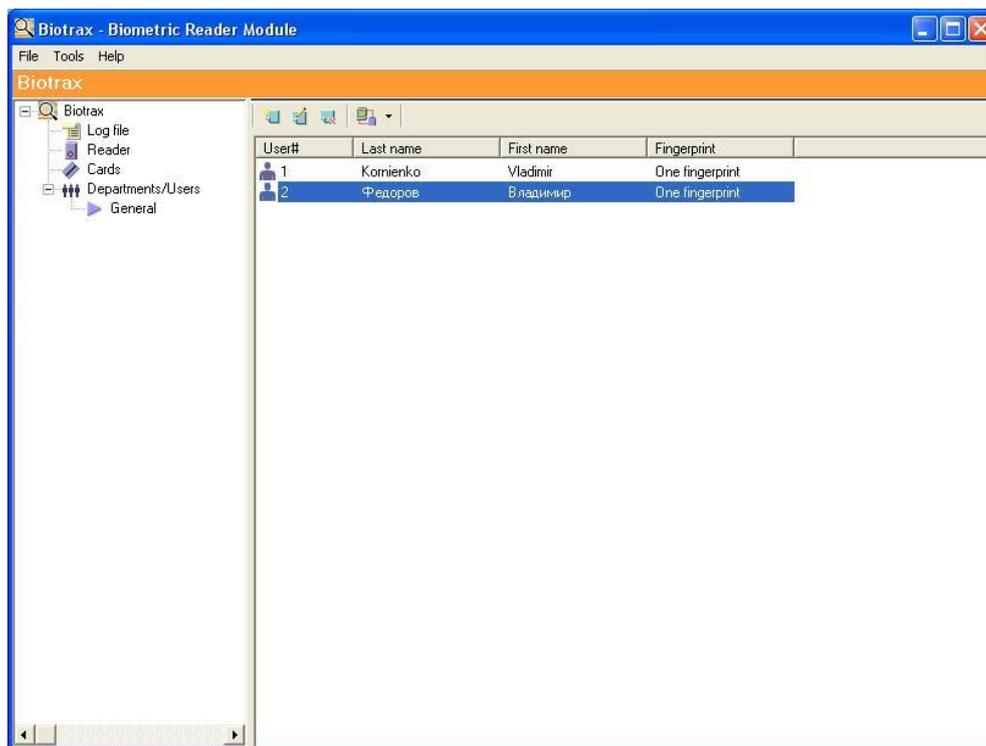


Рис. 1.30. Введенные пользователи биометрической СКУД

1.2.2.2. Программирование устройства в автономном режиме в качестве считывателя с клавиатуры самого считывателя (без подключения к компьютеру)

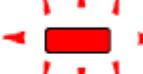
При рассмотрении работы биометрического контроллера/ считывателя в качестве считывателя, как и в режиме работы в качестве контроллера, возможны два режима — нормальный и повышенной безопасности [8, 9], отличия которых можно наблюдать по работе светодиодных индикаторов, что иллюстрируется табл. 1.4.

Различные функции по программированию устройства АУС- W6500 могут быть осуществлены как в режиме программирования, так и в обычном режиме доступа. На этапе изготовления устройства выполнены заводские предустановки, которые можно изменять в процессе эксплуатации устройства, а также вернуть к заводским предустановкам в случае необходимости. Рассмотрим основные настройки, которые необходимо проводить в процессе эксплуатации СКУД такие как смена режимов работы, занесения кодов карт, PIN-кодов доступа и отпечатков пальцев, удаление пользователей из системы. При программировании считывателя с клавиатуры не сто-

ит предпринимать никаких не предусмотренных инструкциями действий, поскольку неправильный ввод кодов и команд может привести к нежелательным последствиям вплоть до потери информации о занесенных пользователях системы, кодов доступа в режим программирования и пр., что повлечет за собой трудоемкий процесс восстановления заводских предустановок и восстановления базы данных пользователей.

Таблица 1.4

Индикация режимов работы устройства

Режим работы	Светодиодный индикатор
<i>Нормальный</i>	 Red
после считывания кода карты или ввода PIN-кода с клавиатуры	 Green
после считывания отпечатка пальца	 Red
если отпечаток пальца не был введен	 Orange
<i>Повышенной безопасности</i>	 Red
после считывания кода карты	 Green
после ввода PIN-кода с клавиатуры (в течение 10 сек)	 Green
после считывания отпечатка пальца	 Red
если отпечаток пальца не был введен	 Orange

Смена режима работы с нормального на повышенной безопасности и наоборот производится с помощью встроенной клавиатуры путем использования специального кода доступа Normal / Secure code, по умолчанию заводская предустановка которого равна 3838, индикатор при этом будет мерцать зеленым цветом. Затем для подтверждения необходимо нажать клавишу «#», и индикатор будет мерцать красным цветом.

Ввод кодов карт и PIN-кодов пользователей осуществляется при входе в режим программирования. Для входа в режим программирования необходим код Programming Code, значение которого по умолчанию равно 1234.

Для ввода кодов существует два метода: стандартный и метод поиска кодов.

Стандартный метод в основном используется при первом занесении данных о пользователе, когда определенному слоту памяти (от 001 до 500) присваивается информация о коде карты доступа и PIN-коде. Для удобства работы следует вести учет пользователей по номеру слота памяти, в который занесена информация о коде карты, PIN-коде, и отпечатке пальца.

Метод поиска кодов применяют в случае, если для пользователя уже занесена информация о коде карты или PIN-коде, и требуется добавить недостающую информацию о PIN-коде или коде карты, а также для занесения информации о второй карте или коде для ранее занесенного пользователя, т.е. в случае, если слот памяти ранее занесенного в систему пользователя не известен.

Порядок действий при использовании стандартного метода следующий:

1. Войти в режим программирования: произвести двойное нажатие клавиши «#» (при этом будет мигать оранжевый светодиод), после чего ввести Programming Code (если код правилен, то оранжевый светодиод будет постоянно гореть).

2. Нажать клавишу «7» для входа в соответствующий пункт меню (включится зеленый светодиодный индикатор).

3. Ввести 3-х значный номер слота памяти (от 001 до 500), если в нем ничего еще не записано, то замигает оранжевый светодиод, приглашая ввести коды доступа (если замигает красный светодиод — это означает, что уже занесена ранее информация о номере карты, но нет информации о PIN-коде, если замигает зеленый светодиод, то это означает, что занесена информация о PIN-коде и нет информации о коде карты доступа, а если раздастся длинный звуковой сигнал — это означает, что выбранный слот памяти уже занят).

4. Ввести в зависимости от необходимости PIN-код и/или код карты доступа (зеленый индикатор перестанет мигать и будет постоянно светиться), что означает приглашение для выбора следующего слота памяти для ввода данных.

5. Выйти из режима программирования путем двойного нажатия клавиши «#» (прозвучат три коротких звуковых сигнала, и загорится красный светодиодный индикатор, извещая о возврате в нормальный режим).

Ввод отпечатков пальцев производится в нормальном режиме доступа (или режиме повышенной безопасности) без входа в режим программирования.

Для ввода отпечатков в нормальном режиме необходимо:

1. Предоставить карту доступа или ввести PIN-код (индикатор замигает оранжевым цветом).

2. Поместить палец на сканер (раздастся короткий звуковой сигнал, сопровождаемый дополнительными тремя короткими сигналами, а также замигает красный светодиод).

3. Повторно приложить палец к сканеру считывателя (прозвучит короткий звуковой сигнал и погаснет светодиодный индикатор, а затем прозвучат три коротких сигнала, свидетельствуя о том, что отпечаток пальца успешно считан).

4. Если прозвучит длинный звуковой сигнал, то процесс ввода отпечатка пальца необходимо повторить.

Удаление информации о пользователе осуществляется двумя методами: стандартным и методом поиска кодов.

При удалении информации стираются из памяти все коды и отпечатки пальцев пользователя, а процесс удаления состоит из следующих этапов:

1. Войти в режим программирования посредством двойного нажатия клавиши «#» (при этом будет мигать оранжевый светодиод), после чего ввести Programming Code (если код правилен, то оранжевый светодиод будет постоянно гореть).

2. Нажать клавишу «8» для входа в соответствующий пункт меню (включится красный светодиодный индикатор).

3. Ввести 3-х значный номер слота памяти (от 001 до 500), если в нем ничего еще не записано, то раздастся длинный звуковой сигнал и устройство будет в ожидании следующего номера слота, а если в данном слоте памяти что-нибудь записано, то замигает зеленый светодиодный индикатор.

4. Ввести Programming Code для подтверждения удаления записи (если код правилен, то прозвучат три коротких звуковых сигнала и последует возврат в нормальный режим, а если программный код не правилен, то прозвучит длинный звуковой сигнал и произойдет возврат в нормальный режим).

Дополнительные возможности программирования устройства в качестве считывателя приведены в табл. 1.5.

Таблица 1.5

Назначение пунктов меню режима программирования

Номер пункта меню	Описание
1	Выбор формата передачи данных PIN-кода: - несколько ключей, 26-бит Wiegand; - один ключ, 6-бит Wiegand (Rosslare формат); - один ключ, 6-бит Wiegand; - один ключ, 8-бит Wiegand

Номер пункта меню	Описание
2	Выбор формата передачи данных кода карты: - 26-бит Wiegand; - Clock & Data
3	Изменение программного кода Program Code
4	Изменение кода выбора режима Secure Code
5	Изменение служебного кода Facility Code (при использовании нескольких ключей)
6	Сервисные установки: - установка блокировки несколько раз неправильно введенного программного кода; - установка подсветки клавиатуры
7	Ввод PIN-кодов
8	Удаление PIN-кодов
0	Возврат заводских предустановок и установка длины PIN-кода

Возможности программирования устройства в режиме работы в качестве контроллера ограничим лишь описанием пунктов меню режима программирования аналогично рассмотренному ранее для режима работы в качестве считывателя с учетом ряда особенностей, приведенных в табл. 1.6.

Таблица 1.6

**Назначение пунктов меню режима программирования
для режима контроллера**

Номер пункта меню	Описание
1	Изменение кода тестирования Test Code
3	Изменение программного кода Program Code

Номер пункта меню	Описание
4	Изменение кода выбора режима Secure Code
6	Сервисные установки: - установка блокировки, сирены и задержки на выход; - установка тревог и вспомогательных функций; - установка блокировки неправильно введенного программного кода; - установка подсветки клавиатуры; - установка вкл/выкл сирены
7	Ввод PIN-кодов
8	Удаление PIN-кодов
0	Возврат заводских предустановок и установка длины PIN-кода

1.2.3. Порядок работы контроллера PERCo-SC-610T/L при управлении одним замком

В варианте «Замок» использования контроллера характеризуется следующими режимами контроля доступа: «ОТКРЫТО», «ЗАКРЫТО», «СИСТЕМНЫЙ КОНТРОЛЬ» и «ОХРАНА». Переключение режимов производится от компьютера. Переключение из режима «СИСТЕМНЫЙ КОНТРОЛЬ» в режим «ОХРАНА» и обратно можно также осуществлять с помощью карт доступа соответствующего статуса.

Переход контроллера из режима в режим сопровождается тремя короткими звуковыми сигналами выносных считывателей. Предъявление карты доступа во всех режимах, кроме режима «ОТКРЫТО», сопровождается звуковым сигналом и кратковременным зеленым свечением индикатора соответствующего выносного считывателя. В режиме «ОТКРЫТО» предъявление карты доступа со-

проводится одним звуковым сигналом и кратковременным выключением зеленого свечения индикатора соответствующего выносного считывателя. Все карты доступа имеют определенные права допуска или статусы:

- разрешенная карта (открывает замок в режиме «СИСТЕМНЫЙ КОНТРОЛЬ»);
- запрещенная карта (не открывает замок ни в каком режиме);
- охрана (разрешенная карта, имеющая возможность постановки на охрану).

Одна и та же карта доступа может иметь одновременно права «доступ» и «охрана».

События, связанные с переключением режимов от компьютера, регистрируются в энергонезависимой памяти контроллера с указанием наименования режима и времени наступления соответствующего события.

Если используются замки с импульсным управлением, то при переходе из режима «ОТКРЫТО» в режимы «СИСТЕМНЫЙ КОНТРОЛЬ», «ЗАКРЫТО», «ОХРАНА» необходимо открыть и закрыть дверь.

Режим «ОТКРЫТО» позволяет контроллеру перевести исполнительное устройство в открытое состояние до подачи другой команды режима от компьютера, при этом выносные считыватели имеют зеленое свечение индикаторов, а проход по картам доступа, обнаруженным в списке разрешённых карт доступа, регистрируется как «Вход» («Выход») с указанием номера карты доступа и времени прохода в энергонезависимой памяти контроллера сразу, если дверь открыта. Если дверь закрыта, то событие «Вход» («Выход») регистрируется после открывания двери в течение времени удержания замка в открытом состоянии.

Проход по разрешённой карте доступа с отклонением от временного графика доступа регистрируется как «Отказ в доступе, нарушение времени» с указанием номера карты доступа и времени прохода в энергонезависимой памяти контроллера при включенной

опции «Контроль времени» сразу, если дверь открыта. Если дверь закрыта, то событие «Отказ в доступе, нарушение времени» регистрируется после открывания двери в течение времени удержания замка в открытом состоянии.

Режим «ЗАКРЫТО» позволяет контроллеру переводить исполнительное устройство в закрытое состояние и удерживать его в этом состоянии до подачи другой команды режима от компьютера. Предъявляемые разрешенные карты доступа не открывают замок, индикаторы выносных считывателей мигают красным светом, а при открывании двери происходит мигание индикатора зелёным светом. Если дверь остаётся открытой более, чем на время разблокировки, считыватели вырабатывают звуковую сигнализацию. Снятие сигнализации осуществляется отменой с компьютера программированием опции «Звуковой сигнал» или закрытием двери.

В случае использования замков с импульсным управлением мигание индикатора считывателей зелёным светом при закрытой двери показывает, что замок открыт. Выносные считыватели вырабатывают звуковую сигнализацию, если дверь или замок остаются открытыми более чем на время разблокировки. Снятие сигнализации в этом случае осуществляется отменой с компьютера, либо закрытием двери, если она была открыта, либо открытием и закрытием двери, если был открыт замок при закрытой двери.

Предъявление любой разрешённой карты доступа регистрируется как «Попытка доступа через заблокированное устройство» с указанием номера карты доступа и времени совершения события.

Режим «СИСТЕМНЫЙ КОНТРОЛЬ» позволяет контроллеру перевести исполнительное устройство в закрытое состояние и удерживать его в этом состоянии до предъявления разрешенных карт доступа со статусом «доступ» или «охрана» одному или обоим выносным считывателям. После предъявления таких карт доступа, контроллер разблокирует исполнительное устройство на время удержания в открытом состоянии. Двукратное предъявление разрешенной карты доступа со статусом «охрана» одному из вынос-

ных считывателей с интервалом не более 5 секунд при закрытой двери (контроллер при этом не должен находиться в локальном режиме «ЗАКРЫТО») переводит контроллер замка в режим «ОХРАНА». В режиме «СИСТЕМНЫЙ КОНТРОЛЬ» возможна работа совместно с пультом дистанционного управления. Тип пульта дистанционного управления программируется от компьютера. Пульт дистанционного управления может представлять собой кнопку (нажатие кнопки обеспечивает разблокирование замка на время удержания в открытом состоянии) или пульт руководителя:

При использовании замков с импульсным управлением переход в режим «ОХРАНА», «СИСТЕМНЫЙ КОНТРОЛЬ» и «ЗАКРЫТО» возможен не только при условии закрытой двери, но и при условии закрытого замка двери.

Выносные считыватели имеют красное свечение индикатора при закрытой двери, отсутствии предъявлений разрешенных карт доступа и нажатий на кнопку дистанционного управления. При предъявлении разрешенной карты или при нажатии на кнопку дистанционного управления доступа индикаторы считывателя имеют зеленое свечение и считыватели производят одиночный звуковой сигнал. При открывании двери происходит мигание индикаторов считывателей зеленым цветом.

В случае использования замков с импульсным управлением мигание индикатора зелёным светом при закрытой двери показывает, что замок открыт.

Если дверь остается открытой более чем на время разблокировки, оба считывателя вырабатывают звуковую сигнализацию. Снятие сигнализации осуществляется отменой с компьютера программированием опции «Звуковой сигнал» при задании конфигурации контроллера или закрытием двери.

В случае использования замков с импульсным управлением оба считывателя вырабатывают звуковую сигнализацию, если дверь или замок остаются открытыми более чем на время разблокировки. Снятие сигнализации в этом случае осуществляется отме-

ной с компьютера, либо закрытием двери, если она была открыта, либо открытием и закрытием двери, если был открыт замок при закрытой двери.

Регистрация событий в режиме «СИСТЕМНЫЙ КОНТРОЛЬ»:

- предъявление карты доступа со статусом «доступ» сразу регистрируется как «Вход» («Выход») с указанием номера карты доступа и времени прохода в энергонезависимой памяти контроллера, если дверь открыта, а если дверь закрыта, то регистрация указанного события производится после открывания двери в течение времени удержания замка в открытом состоянии;

- двукратное предъявление разрешённой карты доступа со статусом «охрана» с интервалом не более 5 секунд при закрытой двери регистрируется как «Пропуск, установлен режим доступа ОХРАНА» с указанием номера карты доступа и времени предъявления в энергонезависимой памяти контроллера;

- попытка прохода по разрешённой карте доступа с отклонением от временного графика доступа регистрируется как «Отказ в доступе, нарушение времени» с указанием номера карты доступа и времени попытки прохода в энергонезависимой памяти контроллера только при включенной опции «Контроль времени».

Режим «ОХРАНА» позволяет контроллеру переводить исполнительное устройство в закрытое состояние и удерживать его в этом состоянии до подачи другой команды режима от компьютера или до перехода в режим «СИСТЕМНЫЙ КОНТРОЛЬ» по двойному предъявлению в течение пяти секунд карты доступа со статусом «охрана» одному из выносных считывателей. При несанкционированной попытке открытия двери контроллер переходит в состояние «ТРЕВОГА».

При использовании замков с импульсным управлением замок может находиться как в закрытом, так и в открытом состоянии. Если замок открыт, то индикаторы выносных считывателей мигают зелёным светом, и выносные считыватели вырабатывают звуковую сигнализацию. При этом в течение 10 секунд с момента перевода

контроллера в режим «ОХРАНА» имеется возможность открыть и закрыть дверь для того, чтобы перевести замок в закрытое состояние. В противном случае по истечении 10 секунд контроллер перейдет в состояние «ТРЕВОГА», если дверь открыта, либо будет продолжать индицировать, что замок открыт.

Двукратное предъявление разрешенных карт доступа со статусом «ОХРАНА» одному из выносных считывателей с интервалом не более 5 секунд переводит контроллер замка в режим «СИСТЕМНЫЙ КОНТРОЛЬ».

Индикаторы считывателей в режим «ОХРАНА» поочередно мигают зеленым и красным, а в состоянии «ТРЕВОГА» индикаторы мигают красным и активизируется выход тревожной внешней сигнализации, а также формируются прерывистые постоянные звуковые сигналы в течение всего времени пока дверь открыта. После закрытия двери состояние тревоги сохраняется в течение десяти минут. Снятие тревоги возможно по команде от компьютера или двукратным предъявлением контроллеру карты доступа со статусом «ОХРАНА» с интервалом не более 5 секунд.

Регистрация событий в режиме «ОХРАНА» осуществляется следующим образом:

- открытие двери регистрируется как событие «Тревога по датчику прохода»;
- предъявления карт доступа без статуса «охрана» регистрируются как «Нарушение режима доступа» с указанием номера карты доступа и времени предъявления в энергонезависимой памяти контроллера;
- снятие тревоги по команде от компьютера регистрируется как событие «Сброс тревоги оператором»;
- двукратное предъявление карт доступа со статусом «ОХРАНА» регистрируется как «Пропуском снят режим доступа «ОХРАНА» с указанием номера карты доступа и времени предъявления в энергонезависимой памяти контроллера.

Независимо от текущего режима работы по команде от компьютера контроллер может быть переведен в состояние тревоги. Состояние тревоги сопровождается световой индикацией, активизацией выхода внешней тревожной сигнализации, а также одновременной звуковой индикацией, формируемой обоими считывателями. Выключение указанной тревожной сигнализации возможно также только по команде от компьютера. При этом также выключается и тревожная сигнализация, инициированная локально, то есть открыванием двери в режиме «ОХРАНА». Выключение тревоги по команде от компьютера регистрируется в энергонезависимой памяти контроллера как «Сброс тревоги оператором».

1.3. Экспериментальное задание

1. Заполнить базу пользователей кодами карт с помощью программно-аппаратного обеспечения PERCo.

2. Заполнить базу пользователей правами управления устройствами, используя программно-аппаратное обеспечение PERCo.

3. Загрузить данные с компьютера в контроллер PERCo-SC-600.

4. Заполнить базу пользователей системы ФИО, фотографиями сотрудников, их биометрическими данными, PIN-кодами доступа и кодами бесконтактных пластиковых карт доступа с использованием данных кодов карт пользователей, полученных при выполнении п. 1, используя программное обеспечение BioTrax и биометрический считыватель.

5. Загрузить введенные данные в считыватель/контроллер BioTrax.

6. Произвести программирование биометрического считывателя в автономном режиме с клавиатуры считывателя, добавив данные новых пользователей системы.

7. Подключить биометрический считыватель к компьютеру, загрузить новые данные из считывателя в базу ПО BioTrax на компьютере и дополнить данные ФИО и фото нововведенных сотрудников.

6. Проверить работоспособность СКУД под управлением компьютера.

7. После выполнения конфигурирования с помощью ПО компьютера проверить работоспособность СКУД в автономном режиме.

1.4. Контрольные вопросы

1. Назвать основные функции, решаемые СКУД.

2. Перечислить основные характеристики используемого оборудования системы контроля доступа Perco серии 600.

3. Назвать основные возможности контроллера замка Perco серии 600.

4. Пояснить принцип работы бесконтактного считывателя с использованием интерфейса Wiegand 26 и объяснить структуру формируемой кодовой посылки.

5. Пояснить особенности подключения и функционирования устройства биометрической идентификации АУС-W6500 производителя Rosslare.

6. Пояснить особенности конфигурирования устройства биометрической идентификации в автономном режиме.

7. Охарактеризовать основные этапы конфигурирования СКУД.

8. Объяснить режим работы контроллера Perco «ОТКРЫТО».

9. Объяснить режим работы контроллера Perco «ЗАКРЫТО».

10. Объяснить режим работы контроллера Perco «СИСТЕМНЫЙ КОНТРОЛЬ».

11. Объяснить режим работы контроллера Perco «ОХРАНА».

2. ПРОЕКТИРОВАНИЕ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ С ПОМОЩЬЮ ПРОГРАММЫ VIDEOCAD

2.1. Цель

Ознакомиться с основными типами видеокамер, структурой их чувствительных элементов, освоить создание проекта на основе трехмерной модели объекта, ознакомиться с настройкой параметров камер и обработкой изображения с помощью программы VideoCad 6.0.

2.2. Краткие теоретические сведения

2.2.1. Сравнительный анализ камер охранного видеонаблюдения

Камеры охранного наблюдения по способу передачи видеосигнала делятся на две группы: аналоговые и сетевые [10]. Аналоговые камеры для передачи сигнала используют коаксиальный кабель, но некоторые из них оснащены встроенным передатчиком видео по витой паре или оптоволокну, что позволяет увеличить расстояние до видеорегистратора без использования промежуточных усилителей.

IP-камеры оцифровывают видеосигнал, сжимают с помощью алгоритмов кодирования MPEG-4, M-JPEG и пр. и передают по витой паре LAN/WAN через сетевой порт Ethernet, а за счет встроенного веб-сервера изображение с них можно просматривать в окне стандартного веб-браузера.

Для любой аналоговой камеры можно найти полноценную замену из группы IP-камер исходя из основных характеристик, ряд из которых выделяет как более предпочтительным промежуточную

разновидность видеокамер — аналоговые видеокамеры высокого разрешения (АHD — analog high definition).

АHD-камерам имеют преимущества по сравнению с известными аналоговыми камерами высокого разрешения по ценовым характеристикам и по совместимости работы в смешанных сетях. Например, преимуществом HD-SDI видеокамер (High-Definition Serial Digital Interface — последовательный цифровой интерфейс высокого разрешения) является более высокое качество изображения Full HD с расширением 1920×1080 , что соответствует 2Мрiх в цифровом формате, но высокая стоимость устройств (камер и видеорегистраторов), сложность настройки и ограничения использования в смешанных сетях не дают широкого применения. Другой пример видеокамер высокого разрешения HD CVI (Composite Video Interface — «композитный видеоинтерфейс для трансляции видео с использованием особого вида аналоговой модуляции) имеет технологию, закрытую для использования другими компаниями, что значительно снижает совместимость с оборудованием других производителей. АHD-И камеры могут без перебоев давать сигнал через коаксиальный кабель, длина которого до 300 метров, но после многочисленных испытаний продемонстрирована способность передавать сигнал на расстояние до 800 метров без применения различных промежуточных усилителей. АHD камеру можно считать гибридным устройством, в котором первоначальная обработка сигналов осуществляется в цифровом виде с дальнейшим преобразованием в аналоговый сигнал. Использование высококачественные КМОП-матриц со сниженным уровнем шумов и процессора обработки изображений (ISP) с отдельной обработкой яркостной и цветовой составляющих видеосигнала, основанной на алгоритмах шумоподавления с поддержкой широкого динамического диапазона WDR, позволяет получить высокое качество изображения при разных уровнях освещённости.

Преимуществом АHD-камер по сравнению IP-устройствами является более низкая стоимость оборудования при аналогичном

качестве и сопоставимом функционале, простота настроек и подсоединения, отсутствие задержек и плавающего изображения, характерных при пакетной передаче данных у цифровых устройств, а также большее расстояние до видеорегистратора без использования промежуточных усилителей.

Основными характеристиками камер охранного видеонаблюдения [10], по которым осуществляется их выбор, являются следующие:

- разрешение;
- фокусное расстояние;
- чувствительность;
- отношение сигнал/шум;
- дополнительные возможности;
- вариант исполнения (уличная, поворотная, купольная, миниатюрная, модульная; безкорпусная).

Разрешающая способность камер составляет, например, 1280×720 или 1920×1080 .

Чем меньше фокусное расстояние, тем больше угол обзора и наоборот. Так, например, при фокусном расстоянии 2,5 мм угол обзора составляет 120° при оптимальном расстоянии распознавания 2 метра, при 4,0 мм — угол обзора 65° оптимальное расстояние распознавания 4 метра, при 12,0 мм — угол обзора 25° , оптимальное расстояние распознавания 12 метров

Чувствительность видеокамер определяет тот уровень освещённости, при котором возможно получение разборчивого изображения. Величина чувствительности, измеряемая в люксах (лк), при использовании видеокамер в дневное и ночное время должна быть не хуже 0,01 лк. Все современные камеры для видеонаблюдения имеют автоматическую регулировку чувствительности, поэтому камера с 0,01 люкс одинаково хорошо покажет и ночную картинку, и изображение при ярком солнечном освещении.

Соотношение сигнал/шум, измеряемый в децибелах (дБ), у хорошей видеокамеры должен быть не менее 45–48 дБ.

К дополнительным возможностям видеокамер относятся наличие инфракрасной подсветки, встроенного микрофона, трансформатора, детектора движений. Переключение режимов день/ночь осуществляется автоматически. Использование инфракрасного фильтра с помощью механического привода перекрывает объектив, препятствуя попаданию избыточного инфракрасного излучения в дневное время, а в ночное время фильтр убирается.

Типы чувствительных элементов — от их типа и качества зависят основные параметры камеры видеонаблюдения, такие как разрешение, чувствительность, динамический диапазон, отношение сигнал/шум, ИК-чувствительность. В настоящее время на рынке представлены камеры наблюдения с ПЗС (CCD) матрицами, с КМОП (CMOS)-матрицами, с PIXIM-матрицами, с тепловизорами, Live-MOS-матрицами.

ПЗС-матрица (прибор с зарядовой связью, англ. charge-coupled devices, CCD) — самый распространенный в настоящее время чувствительный элемент для камер наблюдения. Она представляет собой двумерный массив фотоэлементов, которые накапливают электрический заряд пропорционально падающему на них свету. Эти заряды сдвигаются горизонтально или вертикально и передаются на выходной каскад. А затем начинается накопление заряда для формирования нового видеокадра.

Конструктивно можно выделить две основные схемы матриц: с кадровым переносом и с межстрочным переносом. Также известны схемы, объединяющие межкадровый и межстрочный механизм (строчно-кадровый перенос) при добавлении к ПЗС-матрице межстрочного переноса секции хранения, а также супер-ПЗС (Super CCD), использующие оригинальную сотовую архитектуру, которую образуют восьмиугольные пикселы, позволяя увеличить рабочую поверхность кремниевой подложки, повысить плотность пикселов и увеличить площадь светочувствительной поверхности.

КМОП-матрица (комплементарная ИС металл-оксид-проводник, англ. complementary metal-oxide-semiconductor, CMOS) представляет собой интегральную схему, на которой, помимо собственно светочувствительного элемента, реализованы формирователи тактовых импульсов, логические схемы синхронизации, обработки сигнала и т.д. В ПЗС-камерах все эти элементы реализованы в виде отдельных микросхем, поэтому КМОП-камеры значительно компактнее. В отличие от ПЗС, в КМОП накопленные на пикселях заряды не переносятся, а на ранних стадиях обнаруживаются высокочувствительными усилителями зарядов на КМОП-транзисторах. Технология КМОП, в отличие от ПЗС, позволяет осуществлять большее количество операций прямо на кристалле, на котором расположена фоточувствительная матрица, включая обработку изображения, выделение контуров изображения, уменьшение помех и аналого-цифровые преобразования. Такой широкий набор функций, выполняемых одной микросхемой, сокращает количество необходимых внешних компонентов. Возможность для произвольного доступа к каждому пикселу сенсора по параллельной схеме позволяет считывать сигнал с каждого пикселя или с колонки пикселей напрямую, обеспечивая считывание не только всей матрицы целиком, но и оконное считывание отдельных областей изображения. Наличие дополнительных схем на кристалле КМОП-матрицы приводит к появлению помех, а также тиристорного эффекта. До недавнего времени слабым местом КМОП-камер был высокий уровень шума изображения и низкая светочувствительность, но сейчас эти проблемы успешно преодолены большинством производителей.

PIXIM-матрица — это разновидность КМОП-матриц с отдельным экспонированием пикселей. Она обладает широким динамическим диапазоном, поэтому камеры наблюдения на базе таких матриц формируют сбалансированное изображение с хорошей детализацией и могут использоваться везде, где в кадре присутствуют области с резким перепадом освещенности (окно или открытая дверь). Принцип ее работы базируется на технологии отдельной

экспозиции пикселей Pixim™. В основе этой технологии лежит система высокоточной мультидискретизации, которая в режиме реального времени рассчитывает уровневую коррекцию реакции на освещенность для каждого пикселя матрицы отдельно. Многие производители при изготовлении матриц используют всевозможные модификации технологии PIXIM, поэтому их матрицы могут называться по-другому (SIMD, WDR).

Live-MOS-матрица — разновидность светочувствительных матриц фирмы Panasonic с высокой чувствительностью и качеством изображения даже при высоких углах падения света, с увеличенной скоростью обработки данных, с уменьшением количества управляющих сигналов с 3 в стандартных CMOS сенсорах до 2 (как в CCD-матрицах) увеличило результирующую фоточувствительную область пиксела. Это минимизировало неиспользуемую поверхность датчика. Для уменьшения шумовых характеристик данная технология, разработанная для низковольтных систем 5 В (по спецификации проекта 2,9 В), за счет уменьшенного напряжения питания уменьшает перегрев матрицы, что делает изображения более яркими, менее зернистыми и с низким уровнем белого шума, даже в условиях недостаточной освещенности. Но по ряду характеристик матрица Live-MOS несколько уступает матрице CMOS.

Тепловизор позволяет осуществлять видеонаблюдение в тепловом (инфракрасном) диапазоне. Он может быть построен на основе неохлаждаемой микроболометрической матрицы. При поглощении тепла теплочувствительными элементами матрицы изменяется электрическая проводимость полупроводниковых терморезистивных «мостиков» на основе оксида ванадия, соединяющих теплочувствительные элементы. Электрическая проводимость регистрируется микросхемой, и на основе полученных данных тепловизор формирует картину распределения температуры, которую и видит на экране оператор системы наблюдения. Преимущество тепловизора перед традиционными ПЗС- и КМОП-матрицами состоит в том, что он позволяет видеть объекты в абсо-

лютной темноте и при плохой погоде (при дожде, тумане) и дает оператору достоверную информацию об объектах, находящихся в тени или за листвой деревьев.

Сравнение ПЗС и КМОП. Технологически матрицы КМОП имеют худший коэффициент заполнения, чем матрицы ПЗС — т.е. при том же количестве пикселей на той же площади собственно светочувствительные элементы занимают меньшую площадь и ловят меньше света. Поскольку вокруг них понастроено дополнительные считывающие и передающие информацию элементы для каждого пикселя. В ПЗС-матрице для каждого пикселя такие элементы не нужны, и могут быть вынесены на периферию матрицы или вообще на внешний кристалл. ССD-сенсор лучше снимает в темных местах, а CMOS-сенсор обеспечивает лучшее быстродействие. При использовании ПЗС-сенсора будут лучше цвета и оттенки, больший динамический диапазон, но будет заметна задержка затвора, а применение КМОП-сенсора обеспечивается практически мгновенное срабатывание, но более блеклая картинка или с неестественными цветами при попытках процессора камеры усилить цвета «программно».

КМОП дешевле в производстве, но обладает большим уровнем шума сильнее, чем ПЗС, однако с нарастанием температуры шум, возникающий на ССD сложнее давить — он напоминает зерно, тогда как КМОП-овый шум — это цветастая мозаика.

Таким образом, КМОП лучше тем, что: а) потребляет меньше энергии, б) дешевле стоит в производстве, в) позволяет легче реализовать высокую скорость считывания, в) при повышении скорости не растут «сопутствующие» шумы г) позволяет аппаратно реализовать шумодавление, обеспечивая меньшие шумы при слабом свете, д) на кристалле той же площади можно разместить больше функционала и больше элементарных ячеек, чем на ПЗС-матрице.

ПЗС лучше тем, что: а) при равном разрешении имеет больший коэффициент заполнения, б) имеет меньший уровень шума, в) более точное воспроизведение оттенков и яркостей.

2.2.2. Основы работы в VideoCAD

VideoCAD — многофункциональный и удобный инструмент, предназначенный для профессионального проектирования систем видеонаблюдения, моделирования и измерения параметров видеооборудования и видеоизображений [11–13].

Основные возможности VideoCAD заключаются в следующем [11]:

1. Выбор наиболее подходящих объективов, высот и мест установки видеокамер для обеспечения требуемых параметров зон обзора, обнаружения и опознавания человека, чтения автомобильного номера и получения на экране монитора требуемого размера изображений объекта с известными размерами и местом нахождения.

2. Расчет для нанесения на план объекта реальных размеров горизонтальных проекций зоны обзора, зоны обнаружения человека, зоны опознавания человека и зоны чтения автомобильного номера.

3. Расчет глубины резкости каждой видеокамеры в проекте.

4. Размещение видеокамеры на готовых планировках в форматах *.bmp, *.jpg, *.emf, *.wmf, *.dwg, *.dxf.

5. Экспорт полученных чертёжей в любой из следующих графических форматов: *.bmp, *.emf, *.wmf, *.dxf (R14), *.dxf (R2000).

6. Получение развёрнутой настраиваемой таблицы всех исходных и рассчитанных параметров камер в проекте для экспорта в форматы *.txt, *.csv, *.rtf, *.xls, *.htm.

7. Построение трёхмерных моделей реальной обстановки с возможностью загрузки готовых моделей (человек, автомобиль и др., библиотека может пополняться).

8. Моделирование параметров наблюдаемой сцены с учетом освещения и ограничения видимости.

9. Моделирование светильников с учётом спектра излучения и спектральной чувствительности сенсоров видеокамер.

10. Моделирование параметров видеокамер (спектральная чувствительность; количество пикселей видеосенсора; разрешение; минимальная освещённость при известном отношении сигнал/шум, IRE и апертуре; максимальное отношение сигнал/шум; электронный затвор; АРУ; компенсация встречной засветки; гамма коррекция; камеры день/ночь).

11. Моделирование параметров объективов (фокусное расстояние; диафрагма; APD DC и Video Drive).

12. Моделирование параметров регистраторов (яркость; контраст; компрессия; резкость по горизонтали и вертикали).

13. Получение модели реальной картинки с каждой видеокамеры в проекте.

14. Проектирование интерфейса оператора с помощью Окна мониторов.

15. Расчет длины и электрических параметров кабелей.

При первом запуске программы открывается **Графическое окно**, в котором в двух проекциях отображается одна видеокамера, как показано на рис. 2.1.

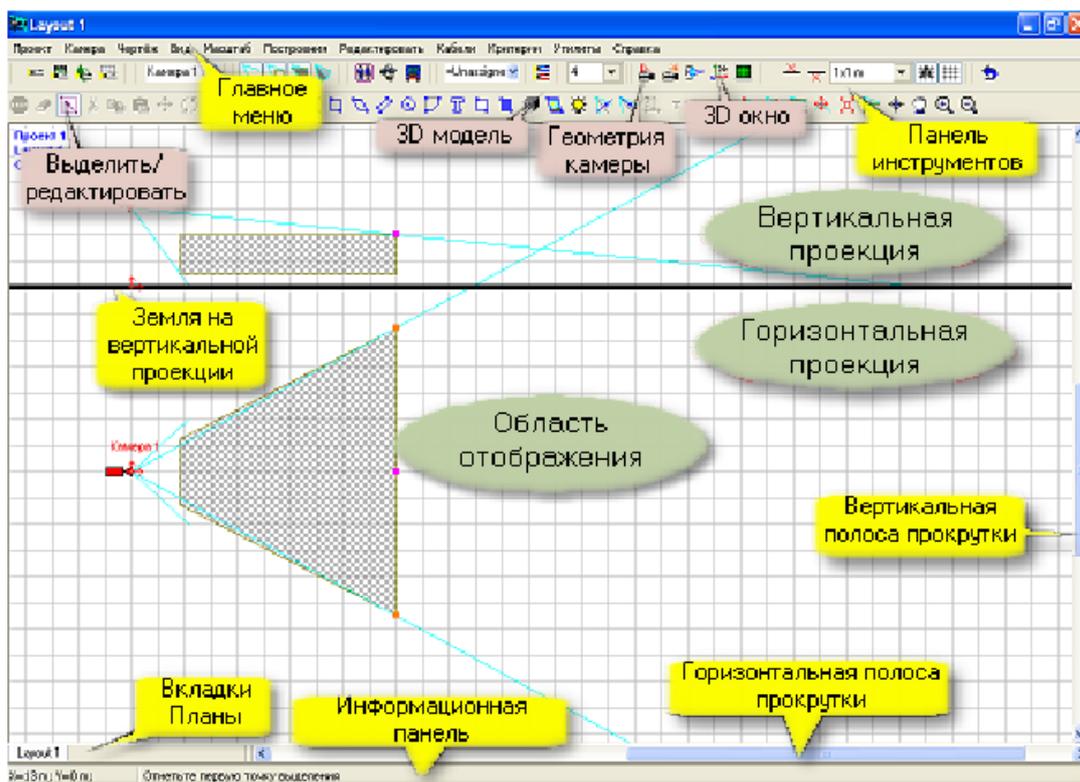


Рис. 2.1. Графическое окно VideoCAD

Передвижение изображения осуществляется нажатием и удерживанием нажатым колёсика мыши, при этом двигается всё изображение, а при одновременном нажатии клавиши **Ctrl** двигается только горизонтальная проекция. Для увеличения какой-либо области на экране используется формируемая с помощью нажатой правой кнопкой мыши область захвата.

Создание проекта происходит автоматически при первом запуске, а последующие проекты создаются из пункта меню, как показано на рис. 2.2.

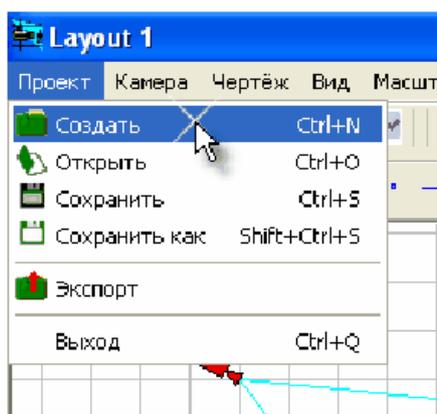


Рис. 2.2. Создание проекта из главного меню проекта

При создании этого простого проекта можно работать только с горизонтальной проекцией, скрыв вертикальную проекцию, кликнув по кнопке на панели инструментов **Скрыть вертикальную проекцию** .

Создание трёхмерной модели обстановки. Для выполнения трёхмерных построений в VideoCAD имеются следующие графические примитивы, которые в окне проекта размещаются с использованием таких инструментов как:

- точка ,
- горизонтальная прямая ,
- вертикальная прямая ,
- отрезок ,
- угол ,
- прямоугольник ,

- наклонный прямоугольник ,
- двойная линия ,
- окружность ,
- дуга .

В трёхмерном пространстве построенные с помощью графических примитивов объекты вытягиваются по высоте, образуя трёхмерные фигуры. Для создания трёхмерной модели необходимо созданным контурам стен, дверей, окон и т. п., выполненным на плоскости в **Графическом окне**, задать значения третьих координат (высот). Минимальные и максимальные высоты, а также цвет получаемых трёхмерных фигур изначально задаются параметрами **типа линии**, которой выполняется построение, но могут быть изменены в процессе построения или позже на **Панели параметров текущего построения**.

Настройка типов линий производится путем выбора в **Главном меню** из пункта **Вид** команды **Настройки** и в появившемся **Окне настроек** на вкладке **Линии** задаются все необходимые ее свойства, как показано на рис. 2.3.

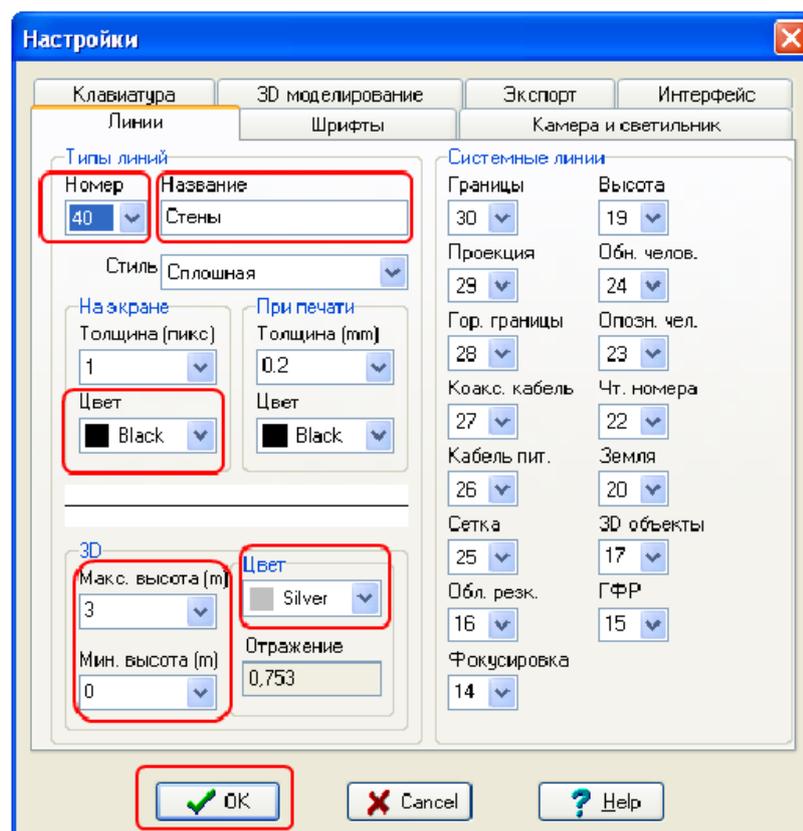


Рис. 2.3. Настройка типов линий

Представленные настройки типа линии выполнены для стен, аналогично можно настроить типы линий 41, 42, 43 для «Дверей», «Столов», «Шкафов» и т.д. Например, для дверей можно выбрать цвет трёхмерной модели «Olive», — 2.2; для стола — цвет трёхмерной модели «Teal», минимальную высоту 0,73, максимальную высоту 0,75 (толщина столешницы 2 см); для шкафов — цвет трёхмерной модели «Maroon», максимальную высоту — 2.

Построение стен осуществляется с использованием инструмента **Прямоугольник** . На появившейся внизу **Панели типа линии** в окошке **Название типа линии** нужно выбрать настроенный на предыдущем шаге тип линии («Стены»), как показано на рис.2.4., а **Панели параметров текущего построения**, в окошке **3D H max** (Максимальная высота 3D построения) появится заданная нами в параметрах **типа линии** высота стен — 3, а нулевое значение в окошке **3D H min** (Минимальная высота 3D построения) означает, что стены будут находиться на земле. Далее необходимо обвести прямоугольниками все стены и колонны на планировке, а окна и двери оставить не обведёнными, и в результате получим план помещения, изображенный на рис. 2.5.

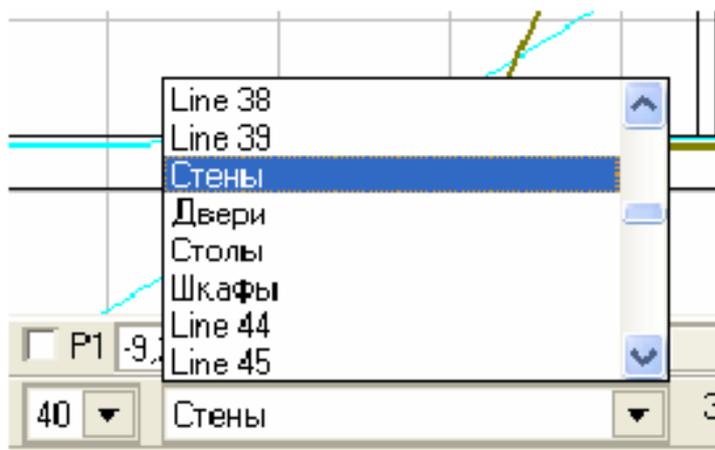


Рис. 2.4. Построение стен

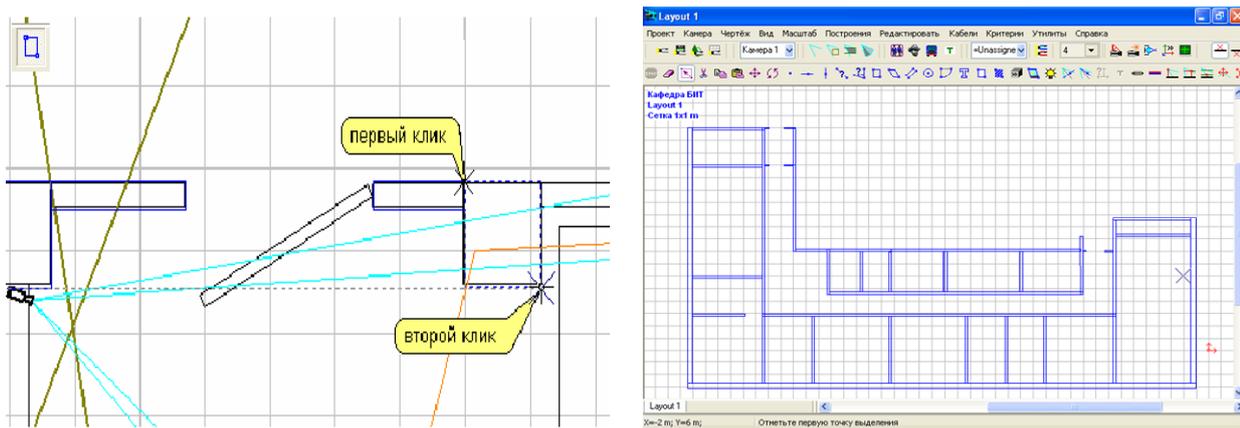


Рис. 2.5. План помещения

Построение окон и дверных проёмов основано на использовании построенных балок, например, для окна — снизу и сверху по балке, которые нужно построить отдельно с помощью инструмента **Прямоугольник** . На появившейся внизу **Панели типа линии** в окошке **Название типа линии** после выбора соответствующего типа линии «Стены» задать на **Панели параметров текущего построения** в окошке **3D Н max** (максимальная высота 3D построения) высоту подоконников — 0,7. Нижняя балка находится на земле, поэтому минимальная высота в окошке **3D Н min** имеет нулевое значение. Затем необходимо построить прямоугольники в оконных проёмах также, как при построении стен. Аналогично строятся **верхние балки окон** в виде прямоугольников поверх нижних балок, при этом перед построением в окошко **3D Н min** (минимальная высота 3D построения) необходимо ввести высоту оконного проёма, равную 2, в окошке **3D Н max** (максимальная высота 3D построения) правильное значение будет равно 3. По аналогии строятся **верхние балки над дверными проёмами** в виде прямоугольников в дверных проёмах путем задания в окошке **3D Н min** (минимальная высота 3D построения) значения высоты дверных проёмов, равной 2,2. В итоге получим изображение объекта охраны с прорисованными оконными и дверными проемами, как показано на рис. 2.6.

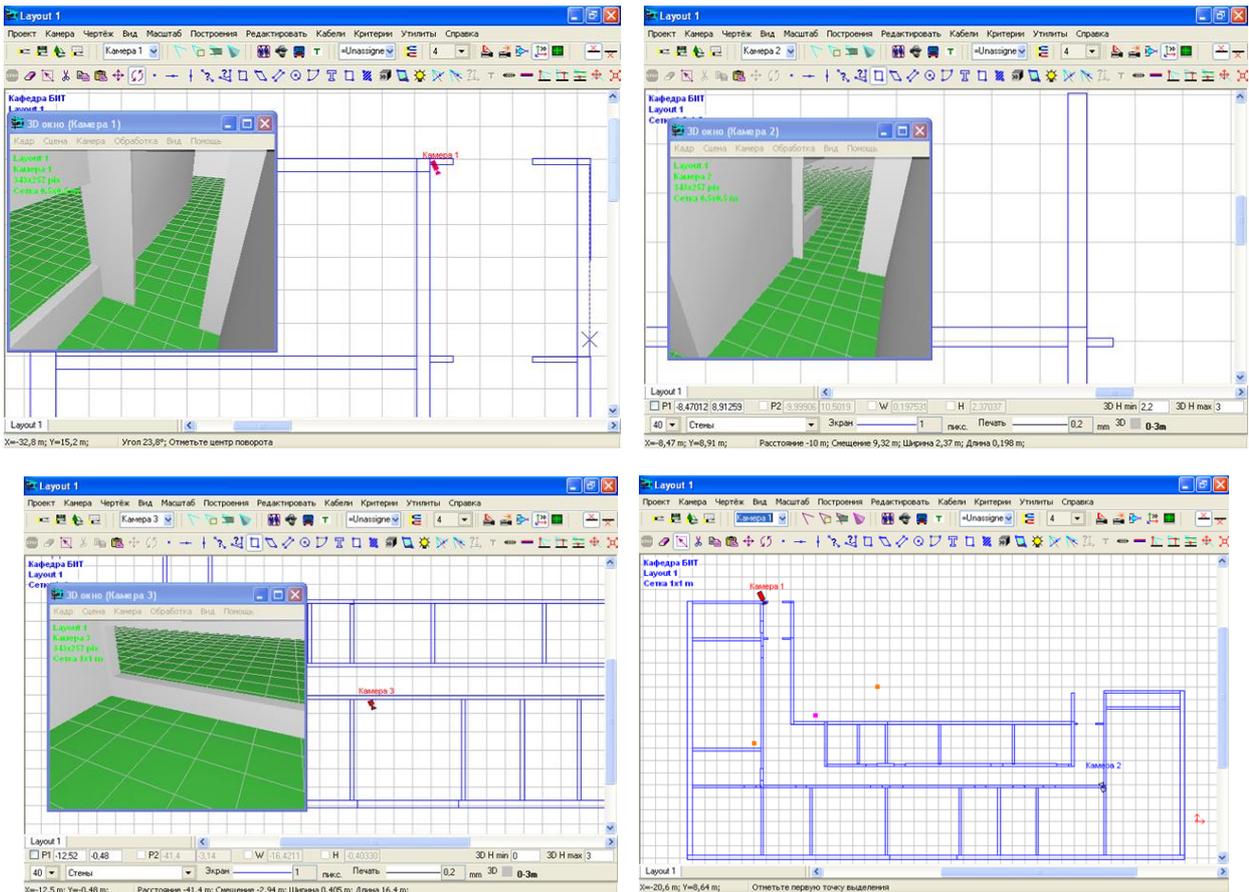


Рис. 2.6. Построение окон и дверных проемов

При проектировании реальной системы видеонаблюдения необходимо разместить в помещениях мебель и другие предметы интерьера, поэтому по аналогии с проведенным описанием производится построение столов и шкафов, как показано на рис. 2.7.

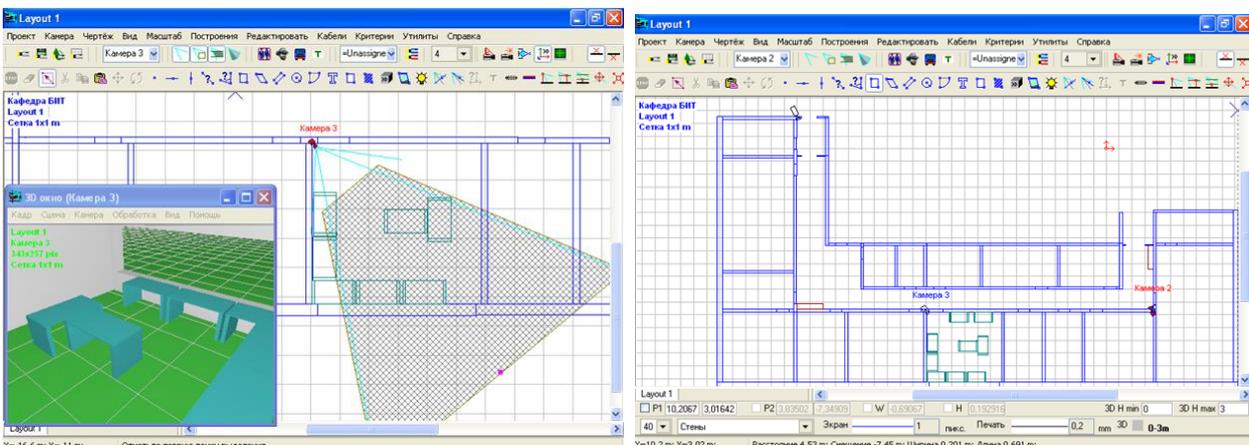


Рис. 2.7. Построение стола и шкафов

Построение дверей осуществляется аналогично типом линии «Двери» в виде прямоугольников, повёрнутый на небольшой угол, для имитации приоткрытой двери с использованием инструмент **Повернуть** , как показано на рис. 2.8.

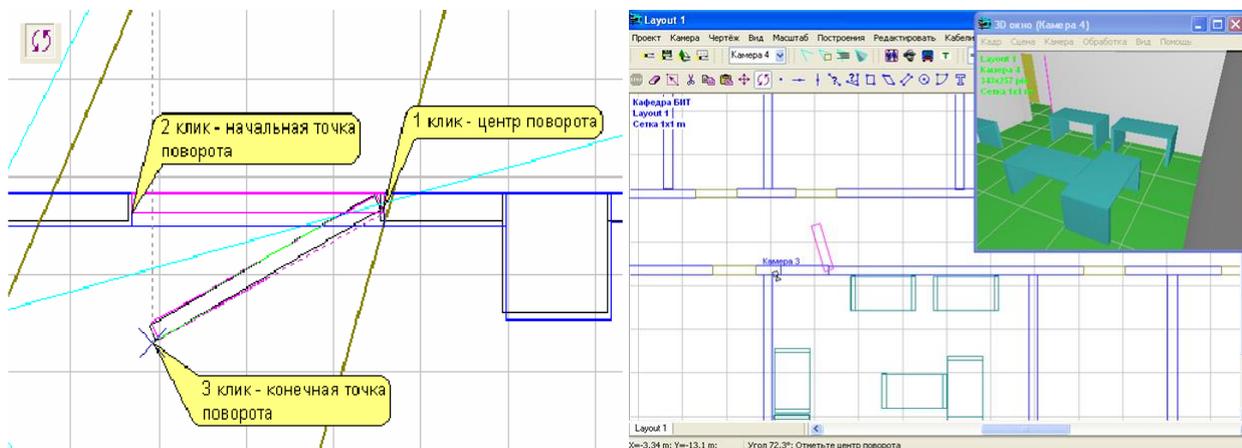


Рис. 2.8. Поворот двери

Размещение готовых 3D моделей на планах помещений осуществляется с использованием инструмента **3D модель**  и выбора соответствующей модели из выпадающего списка с последующим выбором положения и поворота размещенной модели, как показано на рис. 2.9.

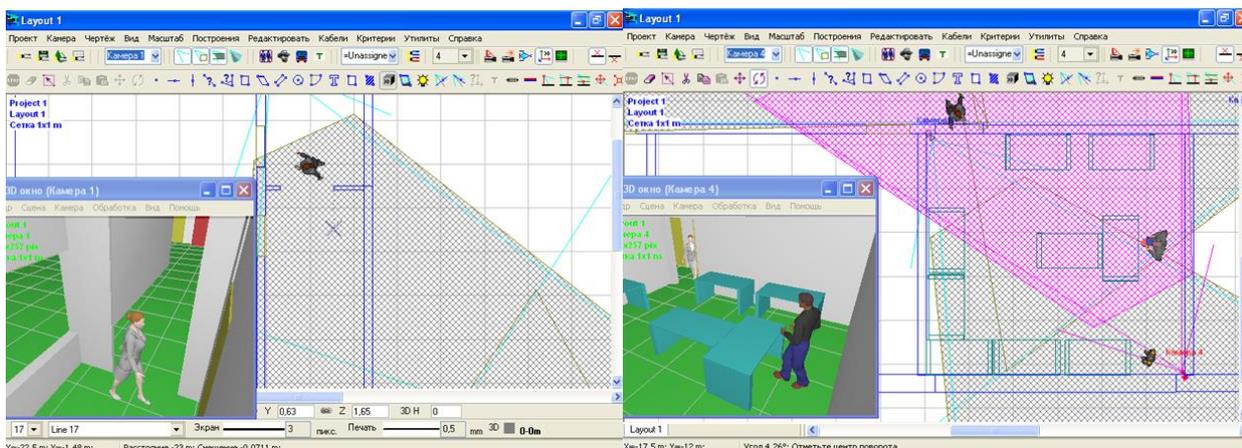


Рис. 2.9. Размещение готовых 3D моделей

Таким образом, после создания трёхмерной модели помещения необходимо загрузить разные камеры и, наблюдая изображения от них в 3D окне, определить какие предметы попадают в зоны обзора, какие предметы затеняют другие, определить мертвые зоны и принять меры к их устранению. На основании этой информации производится корректировка положения и параметров камер. Вначале производится предварительная настройка параметров камер, а затем детализированная настройка их характеристик.

Предварительная настройка параметров камеры производится с использованием инструмента **Геометрия камеры** , окно с параметрами которой приведено на рис. 2.10, где осуществляется выбор **формата видеосенсора** (1/3" — для обычных камер и 1/4" — для миникамер), **высоты установки камеры**, **высоты нижней границы зоны обзора**, **высоты верхней границы зоны обзора**.

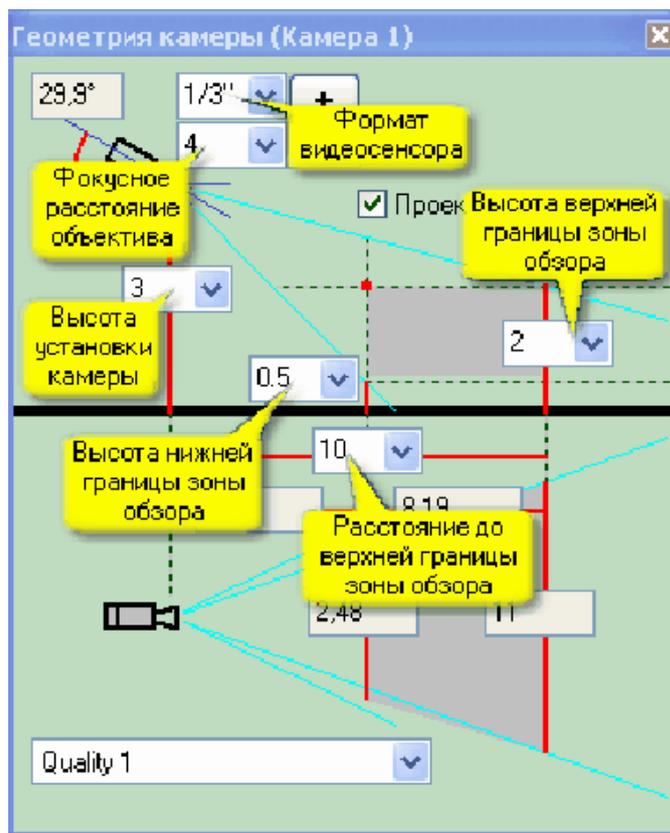


Рис. 2.10. Окно Геометрия камеры

В **Графическом окне** проекта на фоне плана объекта отображается видеокамера вместе с проекцией зоны обзора, рассчитанной согласно заданным параметрам. Кнопки на **панели инструментов**  включают и выключают **отображение границ зоны обзора, границ проекций зоны обзора, штриховку проекций зоны обзора** и отображение зоны обзора в **3D окне** в виде полупрозрачной пирамиды.

Размещение камеры на плане производится при переключении в режим выделения объектов с использованием инструмента **Выделить/Редактировать**  путем захвата сиреневой рамкой объектива видеокамеры и повторного щелчка левой кнопкой мыши для выделения камеры (окрасится в сиреневый цвет), как показано на рис. 2.11.

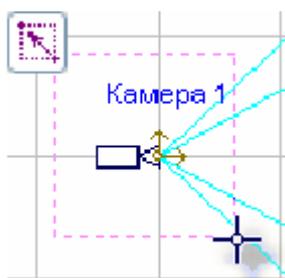


Рис. 2.11. Размещение камеры

Копирование камер производится также в режиме путем последующего выбора инструмента **Копировать** , отметки щелчком мыши **точки привязки копируемых объектов** и вставки с использованием инструмента **Вставить** .

Установка новой камеры осуществляется отметкой щелчком мыши точки установки новой камеры с последующим изменением её названия и описания для неё в появившемся окне создания новой камеры, как показано на рис. 2.12.

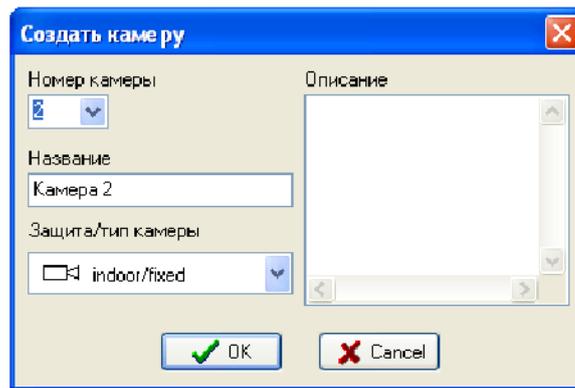


Рис. 2.12. Создание новой камеры

Расстановка камер на плане помещения сопровождается перемещением камер, изменением параметров их зон обзора с целью получения оптимального размещения камер. Ставшие лишними камеры можно удалить после выделения использованием инструмента **Стереть**  или нажатием клавиши **Del** на клавиатуре. В итоге после размещения камер на плане помещения получим требуемый проект системы видеонаблюдения, как показано на рис. 2.13.

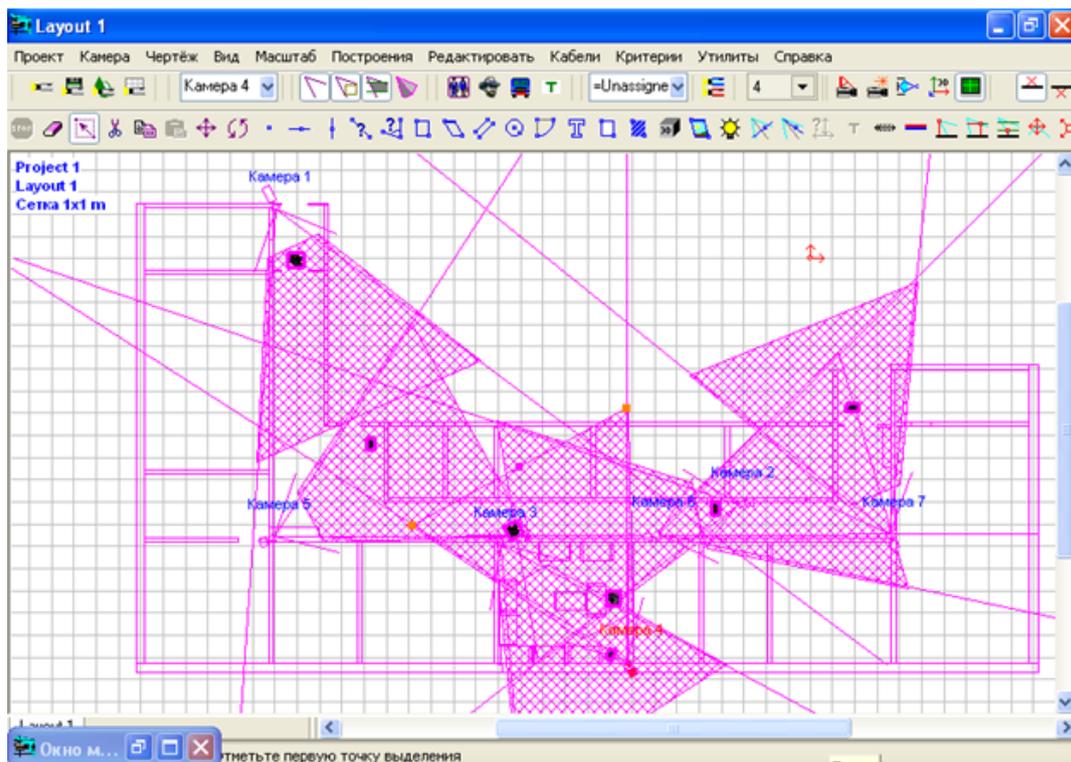


Рис. 2.13. Расстановка камер

Настройка параметров камеры позволяет провести детализированную настройку свойств выбранной камеры путем открытия окна **Чувствительность и разрешение**, с помощью инструмента  на панели инструментов. В данном окне в соответствующих полях для ввода устанавливается цветность, количество пикселей видеосенсора и разрешение, как показано на рис. 2.14.

Настройка параметров обработки изображения осуществляется для выбранной камеры после открытия **3D окна** с помощью инструмента  и двойного щелчка мышкой по **3D окну** для вызова **Панели параметров изображения**, на которой после выбора вкладки **Обработка**, как показано на рис. 2.15, в полях для ввода необходимо ввести **Размер кадра** по количеству пикселей записываемого кадра по горизонтали и вертикали, кроме того установкой флажка в **Одно поле**, можно управлять движками **Яркость** и **Контраст**, **Компрессия** и **Резкость**, после чего сохранить изменённые параметры камеры.

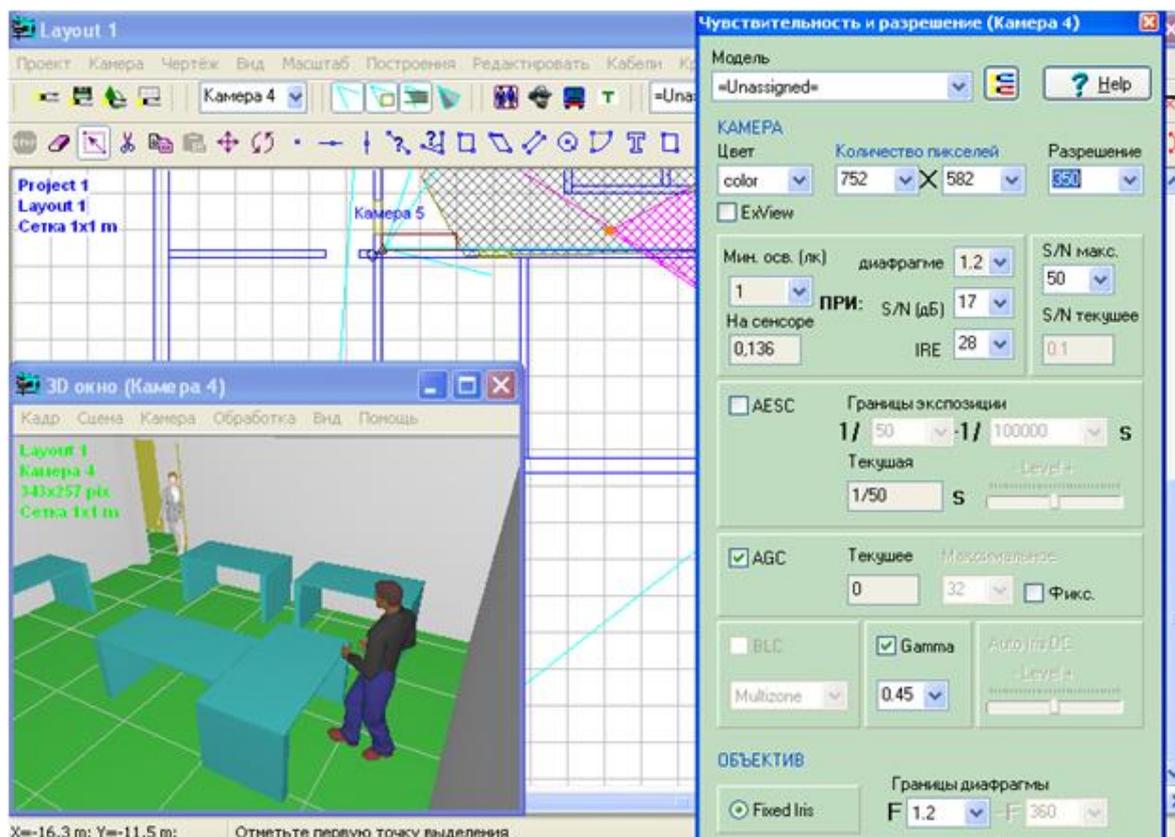


Рис. 2.14. Настройка параметров камеры

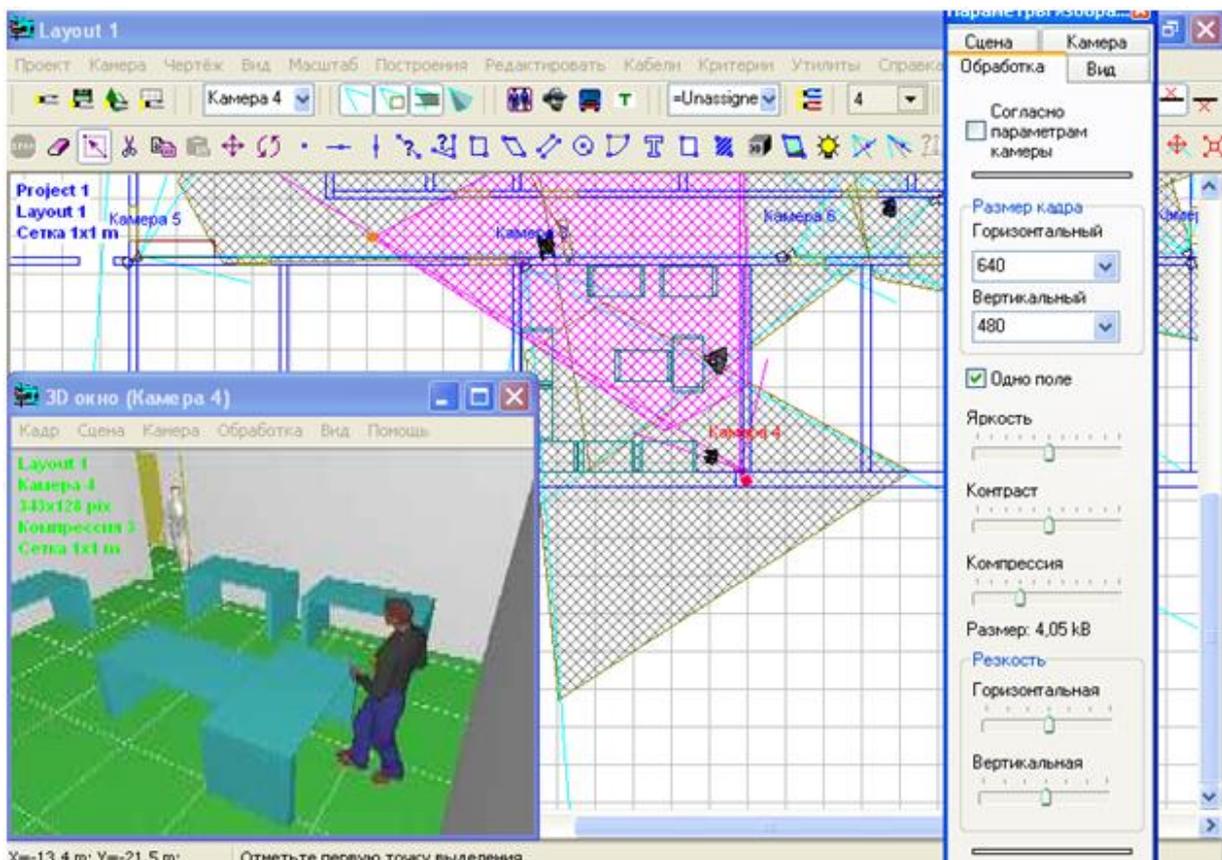


Рис. 2.15. Настройка параметров обработки изображения

Настройка модели монитора осуществляется с помощью инструмента **Окна мониторов** , на панели инструментов которого, как показано на рис. 2.16, по кнопке **Редактировать**  включается **Режим редактирования монитора**, который позволяет в поле ввода ввести **Размерность монитора**, выбрать параметры для одновременного вывода изображений одинакового размера (например, для 3×3 можно одновременно отображать в окне мониторов изображения от 9 камер, а для разработанного проекта — 7 камер), диагональ монитора, отношение сторон экрана.

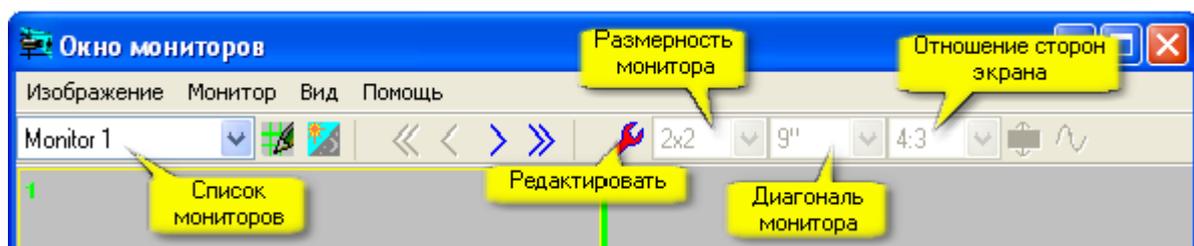


Рис. 2.16. Панель инструментов Окна мониторов

Подключение камер к монитору производится следующим образом: **Графическом окне** необходимо выделить  все камеры, захватив их рамкой выделения, затем перенести курсор на первую (левую, верхнюю) ячейку **Окна мониторов** и щелкнуть левой кнопкой мыши по ней. В результате этих действий появится **3D окно**, в котором автоматически будут последовательно смоделированы изображения от всех выделенных камер, как показано на рис. 2.17.

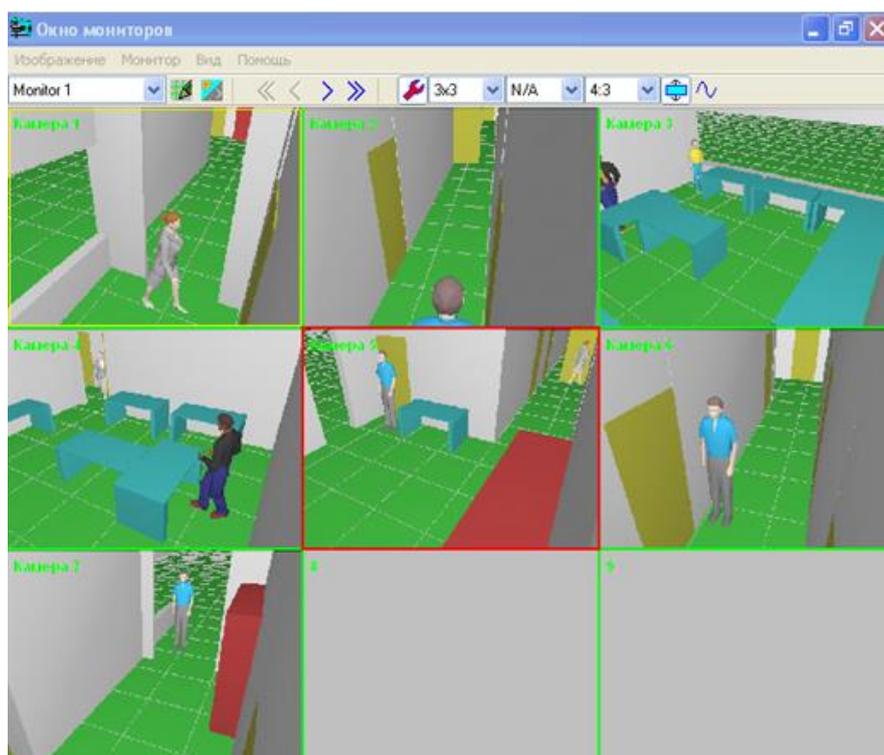


Рис. 2.17. Окно мониторов с подключенными камерами

После настройки монитора и подключения камер необходимо отключить **Режим редактирования монитора** (кнопка **Редактировать**  должна выглядеть отжатой).

Корректировка проекта на основании полученных моделей изображений производится в следующей последовательности:

1. В Окне мониторов произвести двойной щелчок левой кнопкой мыши по изображению от камеры, параметры или размещение которой надо изменить, в результате чего появится **3D окно** с изображением от этой камеры.

2. В **Главном меню 3D окна** выбрать пункт **Вид>Рамка PTZH**, после чего поле зрения в **3D окне** расширится, область действительного поля зрения будет ограничена оранжевой рамкой и по краям изображения появятся кнопки, позволяющие менять положение камеры подобно поворотной камере, фокусное расстояние объектива и высоту установки. PTZ (pan, tilt, zoom)-камеры — это камеры, поддерживающие возможности управления, как аппаратного, так и программного: панорамирования, изменения наклона и фокусного расстояния (зума). Текущие значения параметров в результате настройки будут отображаться рядом с кнопками, как показано на рис. 2.18.

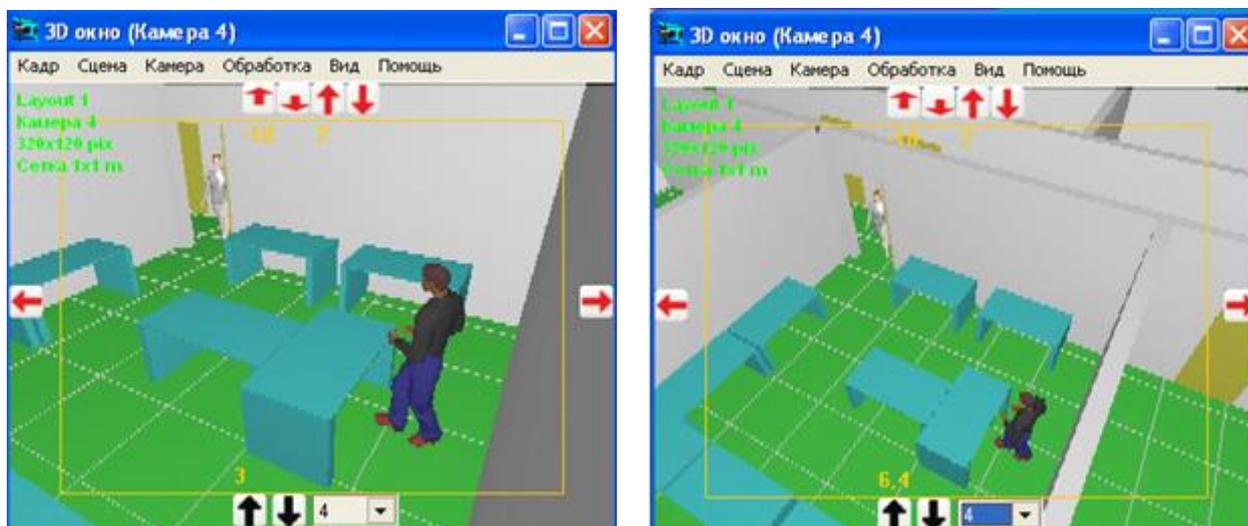


Рис. 2.18. Рамка PTZH в 3D окне

3. Пользуясь этими инструментами настройки камеры будут скорректированы автоматически и на плане в **Графическом окне**.

4. При необходимости переноса камеры на плане необходимо щелкнуть правой кнопкой мыши по изображению в **Окне мониторов** и выбрать в контекстном меню **Найти на плане**, после чего данная камера будет выделена и показана на плане в **Графическом окне**. Для перемещения камеры необходимо подвести курсор точно к объективу выделенной камеры, нажать левую кнопку мыши, переместить курсор на новое место и отпустить левую кнопку.

5. После изменения положения камеры требуется обновить изображение от неё на мониторе посредством щелчка правой кноп-

кой мыши по изображению от изменённой видеокамеры в **Окне мониторов** и выбора в контекстном меню команды **Обновить**.

6. При необходимости можно создать новые камеры, копированием существующих, а затем подключить их к монитору. Для подключения новой камеры к монитору следует выделить камеру на плане, включить **Режим редактирования монитора** и щелкнуть по ячейке, в которой должно отображаться изображение от этой камеры.

Более подробно ознакомиться с функциями VideoCAD можно из технической документации, размещенной на сайте разработчика [11].

2.3. Экспериментальное задание

1. Создать проект системы видеонаблюдения для выбранного помещения.

2.4. Контрольные вопросы

1. Охарактеризовать основные виды камер систем охранного видеонаблюдения, привести их достоинства и недостатки.

2. Перечислить основные характеристики камер охранного видеонаблюдения

3. Сравнить различные типы чувствительных элементов систем видеонаблюдения.

4. Перечислить достоинства и недостатки ПЗС- и КМОП-сенсоров.

5. Описать основные характеристики программы VideoCAD.

6. Пояснить основные этапы построение трехмерной модели охраняемого помещения.

7. Каким образом производится настройка параметров видеокамер и их расстановка на плане помещения?

8. Как осуществляется настройка параметров обработки изображения?

9. Пояснить настройку параметров системы отображения видео.

10. Как осуществляется корректировка проекта системы видеонаблюдения на основании полученных моделей изображений от камер?

3. ИЗУЧЕНИЕ ОСНОВНЫХ ХАРАКТЕРИСТИК БЕСПРОВОДНОЙ ОХРАННОЙ СИГНАЛИЗАЦИИ «OASIS»

3.1. Цель

Ознакомиться с составом оборудования системы охранной сигнализации и изучить возможности центрального блока системы — приемно-контрольного прибора.

3.2. Краткие теоретические сведения

Система беспроводной охранной сигнализации «Оазис» имеет следующие основные технические характеристики [14, 15]:

- рабочая частота 868 МГц;
- дальность действия — до 600 м на открытом пространстве;
- 50 беспроводных устройств в составе системы;
- 4 проводные зоны;
- 50 кодов доступа встроенного считывателя RFID карт;
- 2 уровня частичной постановки с задержкой на выход по разделам;
- управление домашней автоматикой;
- скрытый беспроводный магнитоконтактный извещатель;
- литиевые батареи со сроком службы до 3 лет;
- контроль через ПО COMlink.

Список основного оборудования приведен в табл. 3.1 устройств системы, а порядок установки приведен на рис. 3.1.

Состав основного оборудования системы ОАЗИС

№	Название устройства	Описание
1	Контрольная панель	До 50 адресов внешних устройств (извещатели, брелки, клавиатура, сирена, термостат, домашняя автоматика и пр.), до 50 кодов карт, 3 раздела, выход на проводную клавиатуру, выходы на внутренний и внешний световой/звуковой оповещатели 2 программируемых выхода, 4 проводные зоны Коммуникактор LAN и ТКК, коммуникатор GSM, голосовой модуль, интерфейсный кабель
2	Пульт управления со встроенным считывателем	Беспроводной/проводной, считыватель RFID
3	Извещатель охранный пассивный инфракрасный объемный	Зона обнаружения 112 кв.м., цифровая обработка сигнала, высокий уровень помехозащищенности
4	Совмещенный извещатель охранный пассивный инфракрасный и разбития стекла	Цифровая обработка сигнала, высокий уровень помехозащищенности
5	Магнитоконтактный извещатель двери	Имеет вход для подключения внешних извещателей
6	Магнитоконтактный извещатель скрытый для окон	Для окон евро стандарта

№	Название устройства	Описание
7	Сирена для помещений	Питание от сети, индикация тревог, задержек на вход/выход, дверного замка, сигналов извещателей
8	Внешняя сирена	Датчик вскрытия корпуса
9	брелок	2 или 4 кнопочный, управление релейными модулями
10	Кнопка дверного звонка	Подача сигнала паники, управление релейными модулями
11	Уличная клавиатура	Встроенный считыватель карт, проводное подключение к контрольной панели
12	Беспроводной термостат	Управление релейными модулями
13	Релейный модуль выходов	2 управляемых по радиоканалу реле, питание 12В или от сети
14	Пожарный извещатель	Комбинированный дымовой и тепловой, встроенная сирена, функция самоконтроля
15	Извещатель утечки газа	Реагирует на газ и пар, питается от сети
16	Миниатюрный объемный извещатель	Для салона автомобиля
17	Миниатюрный извещатель разбития стекла	Для салона автомобиля, дальность действия до 9 м
18	Модуль голосовой связи	Прослушивание помещения, связь с зарегистрированными в системе телефонами
19	Модуль управления для автомобиля	Устанавливается в автомобиле, питается от бортовой сети с подключаемыми извещателями, позволяет управлять светом фар, звуковым сигналом и пр.



Рис. 3.1. Порядок установки оборудования

Архитектура контрольной панели имеет модульную структуру, как показано на рис. 3.2, и позволяет производить расширение простым добавлением таких модулей как модуль радиоприемника на 50 беспроводных зон, модуль расширения проводных зон с 10 входами, расширяющий контрольную панель до 14 проводных зон, GSM коммуникатор, позволяющий передавать сообщения пользователю, извещения на станцию мониторинга, управлять системой с клавиатуры телефона через GSM канал или через Интернет с сайта GSMLink, коммуникатор LAN/PTSN, позволяющий передавать сообщения по проводным линиям LAN (Ethernet) и по телефонной линии и управлять системой дистанционно с клавиатуры телефона или через Интернет с сайта GSMLink, голосовой телефонный коммуникатор, позволяющий передавать голосовые сообщения [14].

Проводные и беспроводные устройства используют одинаковые адреса (номера зон). Диапазон адресов для проводных зон: 01–04 или 01–14, для беспроводных зон: 01–50. Контрольная панель не позволяет одновременного использования проводных и беспроводных зон с одним адресом, поэтому при использовании проводной зоны автоматически отключается беспроводная зона с таким же адресом. Дополнительные проводные зоны имеются на беспроводных устройствах: пульте управления, дверном магнито-контактном извещателе и объемном ИК извещателе.

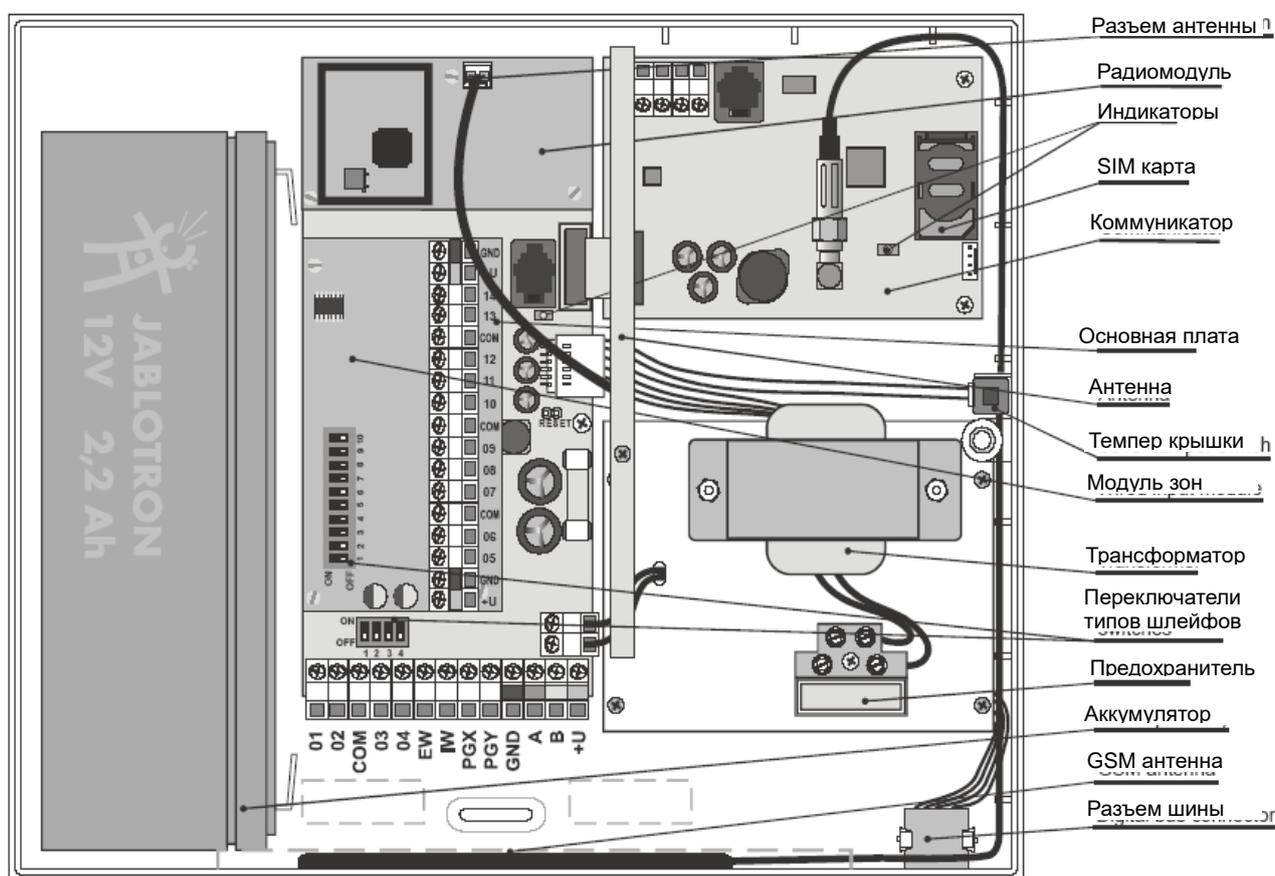


Рис. 3.2. Внутреннее содержимое контрольной панели

Беспроводные устройства группируются в три раздела: **А**, **В** или **С**, назначение которых влияет на режимы охраны, например, **А** — дневной режим, **АВ** — ночной режим, **АВС** — полная охрана) или система может быть разбита на независимые разделы **А** и **В** и общий раздел **С**. Если разделы **А** и **В** поставить на охрану незави-

симо, то раздел С ставится на охрану автоматически после постановки обоих разделов.

Контрольная панель имеет два выхода тревоги на внутреннюю сирену и на внешнюю сирену, как показано на рис. 3.2. Если не подключены к этим выходам проводные оповещатели, то оба тревожных канала будут беспроводными при зарегистрированных в системе внутренней и внешней сирен. В системе может быть 5 видов тревоги: охранная, темпер, пожар, паника и техническая тревога.

Два программируемых выхода PGX и PGY позволяют подключить проводные исполнительные устройства, например, электромагнитный замок и пр., но если проводные устройства не задействованы, то данные выходы могут быть беспроводными при использовании приемников беспроводных релейных модулей выходов.

Управление системой можно осуществлять с помощью кодов пользователей, карт пользователей, брелоками, а также по телефону или через Интернет, если в контрольной панели установлен коммуникатор. При разбиении на разделы возможно назначение кодов и карт разделам для каждого из 50 пользователей системы. Для повышения уровня безопасности при постановке на охрану или снятии с охраны картами и кодами можно задать подтверждение карты кодом.

Режимы работы контрольной панели следующие: *рабочий, обслуживания и настроек*. Рабочий (пользовательский) режим предназначен для ежедневной работы с системой пользователей при постановке на охрану, снятии с охраны, управлении автоматикой и пр. Режим обслуживания предназначен для администратора, использующего мастер код для осуществления частичное программирования системы, например, при программировании кодов пользователей. Режим настроек предназначен только для установщика и используется для регистрации беспроводных устройств, программирования параметров системы и пр.

Система Oasis позволяет защищать автомобиль, припаркованный возле дома. Модуль управления для автомобиля, зарегистрированный в свободный адрес контрольной панели, можно подключить к автосигнализации, и тревога автосигнализации будет индцироваться как тревога Паника. Если на автомобиле нет сигнализации, в нем можно установить извещатели и назначить их отдельному разделу.

Подключение оборудования в состав системы начинается, как показано на рис. 3.1, с включения *приемно-контрольной панели*, в которой предварительно необходимо подключить необходимые модули, а при использовании проводных устройств их предварительно необходимо подключить к соответствующим выходам, как было указано ранее для выхода на внутреннюю сирену IW и выход на внешнюю сирену EW, для релейных выходов исполнительных устройств PGX и PGY. Кроме того для проводных шлейфов сигнализации, в которые подключаются проводные извещатели, входы 01–04 должны использовать оконечные резисторы в нормальном состоянии номиналом 1 кОм для определения состояния шлейфа, как показано на рис. 3.3. В одном шлейфе можно использовать до 5 извещателей с нормально замкнутыми контактами, причем извещатели должны быть включены последовательно и иметь параллельно подключенные резисторы. Нормально замкнутые температурные контакты соединяются последовательно без резисторов. Количество температурных контактов не ограничено, они могут комбинироваться с тревожными выходами извещателей (с параллельными резисторами). При использовании проводных зон соответствующий переключатель типа зоны ON/OFF на плате контрольной панели должен быть включен в положение ON.

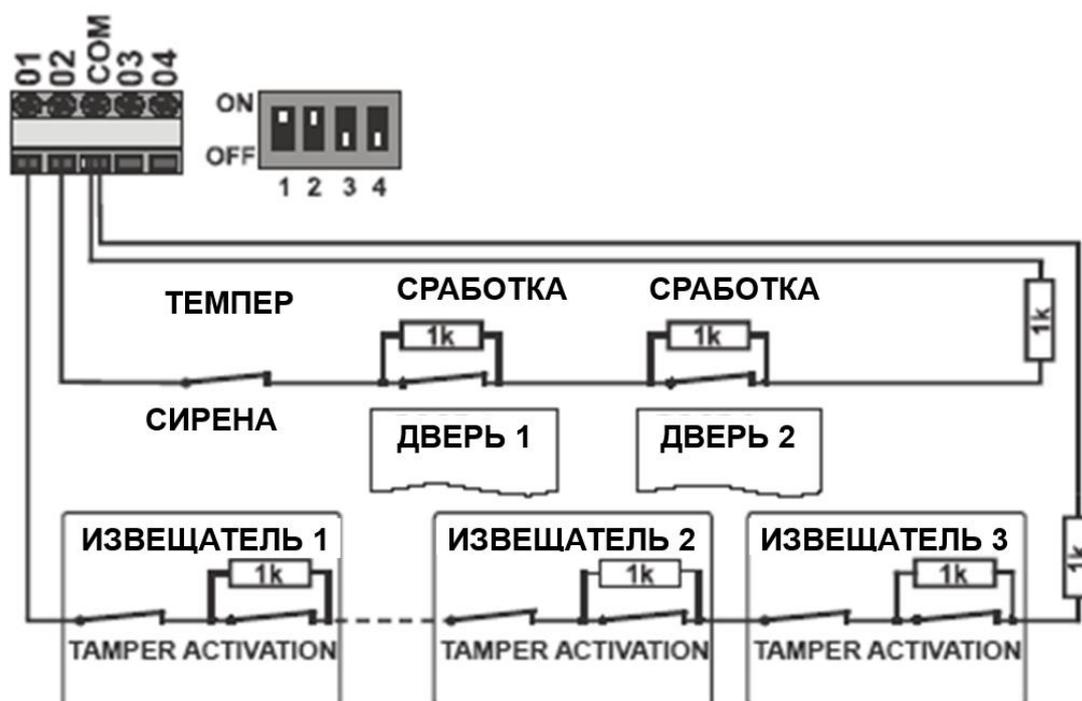


Рис. 3.3. Подключение проводных извещателей к контрольной панели

Проводной пульт позволяет управлять контрольной панелью и программировать как ее свойства, так и свойства всех подключенных устройств. Проводной пульт может быть подключен к контрольной панели или с помощью кабеля длиной до 10 м через RJ разъем, или с помощью витой пары (до 100 м), подключенной к клеммам цифровой шины (GND, A, B, +U), как показано на рис. 3.4.

При регистрации в контрольной панели беспроводного пульта [15] необходимо выполнить следующие действия:

1. Открыть пульт.
2. Убедиться в мигании зеленого индикатора панели.
3. Замкнуть переключку Reset на контрольной панели на 1 секунду для входа в режим регистрации.
4. Установите батарейки в пульт.
5. Пульт выдаст звуковой сигнал и зарегистрируется по адресу 05 (или 15) с выдачей сообщения на индикаторе «Enrollment 06: Device» (или «Enrollment 16: Device»).
6. Нажать кнопку # для перехода из режима регистрации в режим программирования.

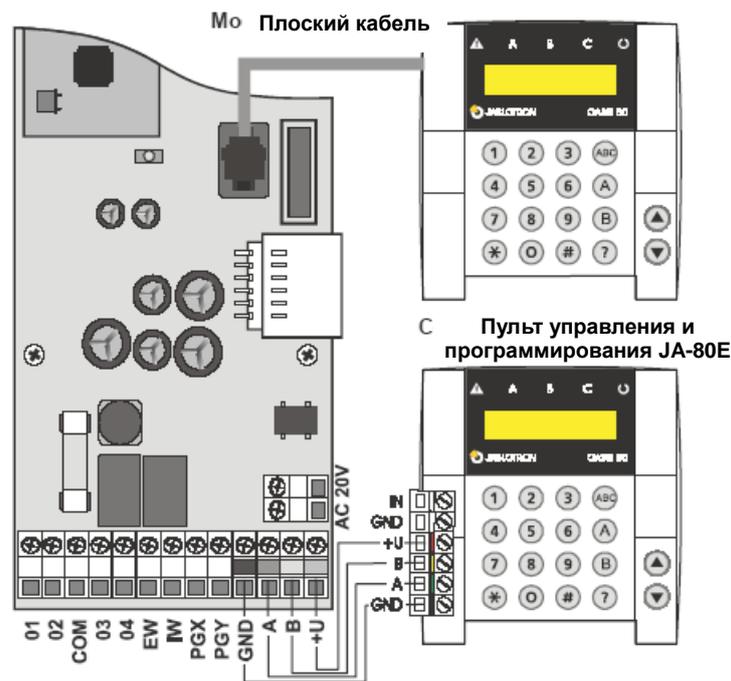


Рис. 3.4. Подключение пульта управления к контрольной панели

После регистрации пульта управления на его экране отображается встроенное меню, в котором легко разобраться и выполнить, например, выбор языка, даты, времени и пр.

При работе в режиме настроек потребуется знать Мастер код (по умолчанию 1234) и код установщика (по умолчанию 8080), вводимые с клавиатуры пульта управления.

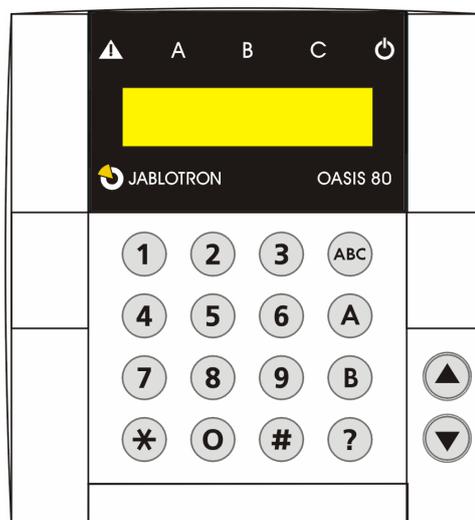


Рис. 3.5. Органы управления и индикации пульта управления

Индикаторы пульта управления, внешний вид которого приведен на рис. 3.5, имеют следующие назначения:

А, В, С — индикаторы статуса разделов — если все разделы на охране, включены все индикаторы (А, В и С);

0...9 — кнопки ввода цифр;

***** — ввод команд;

— выход из режима;

АВС — постановка системы на охрану (все разделы А, В и С);

А — постановка на охрану раздела А (частичная постановка);

В — постановка на охрану раздела В (частичная постановка);
в системе с разделами кнопка В ставит на охрану раздел В, а раздел С ставится на охрану, если А и В на охране;

? — Индикация сработавших извещателей, сбои и статус PGX/PGY;

▲ — листание в меню; включение первого релейного выхода, если он запрограммирован для этого;

▼ — листание в меню; выключение первого релейного выхода, если он запрограммирован для этого.

Регистрация беспроводных устройств ограничена 50 адресами (01–50) и выполняется в следующей последовательности:

1. Контрольная панель должна быть в режиме **настройки**, вход в который производится набором команды ***0 код установщика** (заводская установка: 8080), при этом контрольная панель должна быть снята с охраны;

2. Для входа в режим регистрации необходимо нажать кнопку **1**, после чего на индикаторе будет показан первый свободный адрес;

3. Используя кнопки **▲** и **▼** для выбора желаемого адреса необходимо перейти к нему, и если адрес уже занят, это индицируется символом **А**;

4. Устройство будет зарегистрировано по выбранному адресу сразу после установки батарей или подачи питания;

5. После регистрации включается символ **A** и предлагается следующий свободный адрес.

6. Поочередной установкой батарей во все беспроводные устройства происходит их регистрация.

7. Для выхода из режима регистрации следует нажать кнопку **#**.

При регистрации беспроводных устройств по адресу 01–04 происходит отключение соответствующей проводной зоны, а если беспроводное устройство удаляется из адресов 01–04, тогда проводная зона снова начинает работать. Регистрация брелоков осуществляется нажатием и удержанием пары кнопок одновременно **6+6** что позволяет зарегистрировать 4-кнопочный брелок дважды но по двум разным адресам с разными функциями пар кнопок. При невозможности зарегистрировать устройство в контрольную панель даже при свободном адресе необходим уверенный прием сигнала, для этого необходимо либо сократить расстояние между контрольной панелью и устройством, либо располагать его не слишком близко — не менее 2 метров.

Измерение уровня сигнала необходимо производить для проверки надежности работы устройств в системе в следующей последовательности:

1. Контрольная панель должна находиться в режиме настройки, вход в который осуществляется вводом команды **0 код установщика (заводская установка 8080)*, причем контрольная панель должна быть снята с охраны.

2. Набрать на клавиатуре команду **298**, после чего появится младший адрес зарегистрированного устройства.

3. После выбора устройства в указанном адресе пульт покажет уровень сигнала в диапазоне от 0/4 до 4/4.

4. Выход из режима осуществляется нажатием кнопки **#**.

Для измерения сигнал от внутренней сирены используется кнопка на ее корпусе, а для измерения сигнала от уличной сирены — открывание ее крышки (активизация темпера).

Каждое установленное устройство должно иметь уровень сигнала не менее 2/4. Если сигнал слишком слабый, устройство следует переместить, или включить повышенный уровень чувствительности приемника контрольной панели. Наиболее удобный способ измерения уровня сигнала — через ПО OLink, установленное на компьютере.

Удаление зарегистрированных устройств, если возникает необходимость, производится в следующей последовательности:

1. Контрольная панель должна находиться в режиме настройки, вход в который осуществляется вводом команды *0 код установщика (заводская установка 8080), причем контрольная панель должна быть снята с охраны.

2. Набрать на клавиатуре **1** для входа в режим регистрации, после чего используя кнопки со стрелками произвести выбор адреса удаляемого устройства.

3. Нажать и удерживать кнопку **2** до звукового сигнала, после чего символ **A** должен выключиться.

4. После удаления выбранного устройства осуществить выход из режима нажатием кнопки **#**.

Регистрация контрольной панели в беспроводных модулях релейных выходов позволяет использовать сигналы выходов контрольной панели PGX и PGY для управления автоматикой и осуществляется следующим образом:

1. Контрольная панель должна находиться в режиме настройки, вход в который осуществляется вводом команды *0 код установщика (заводская установка 8080), причем контрольная панель должна быть снята с охраны.

2. На модулях релейных выходов необходимо включить режим регистрации.

3. Набрать команду **299** на пульте контрольной панели и убедиться, что индикаторы модуля мигнули несколько раз для подтверждения регистрации.

Контрольную панель можно зарегистрировать в любое количество беспроводных модулей релейных выходов, но в каждый из модулей можно зарегистрировать только одну контрольную панель. Каждый модуль имеет два выходных реле X и Y, регистрируемых индивидуально. Реле X может работать по сигналу PGX, а реле Y может работать по сигналу PGY, регистрируемых соответственно.

Программирование контрольной панели проще всего осуществлять с помощью ПО OLink с ПК, но можно программировать с пульта командами согласно табл. 3.2, учитывая уже известную последовательность действий — войти в режим настроек командой **0 код установщика (заводская установка 8080)*, ввести соответствующую команду и выйти из режима настроек нажатием кнопки #.

Систему можно ставить на охрану и снимать с охраны кодом, брелоком или удаленно по телефону или через Интернет или с ПК через ПО OLink.

Сброс контрольной панели выполняется в случае возникновения необходимости вернуть контрольную панель к заводским установкам и выполняется в следующей последовательности:

1. Отключить сетевое питание.
2. Установить переключку RESET.
3. Подключить аккумулятор и сетевое питание.
4. Подождать, пока зеленый индикатор начнет мигать, после чего снять переключку RESET.

Команды программирования контрольной панели

Функция	Команда	Опции	Завод. установка	Примечания
Вход в режим регистрации	1	удержание 2 = удаление устройства с индицируемым адресом; удержание 4 = удаление устройств из всех адресов; # = выход из режима регистрации	Нет устройств	Устройства регистрируются подачей питания, брелки — нажатием и удержанием пары кнопок. Занятый адрес индицируется символом А. Регистрация устройства по новому адресу переносит его из старого адреса
Время задержки на выход	20х	$x = (1-9) \times 10 \text{ сек} = 10-90 \text{ сек}$	30 сек	Для функции входной двери умножается на 30 сек. (от 30 до 270 сек)
Время задержки на вход	21х	$x = (1-9) \times 5 \text{ сек} = 5-45 \text{ сек}$	20 сек	
Длительность тревоги	22х	$x = 1-8 \text{ (мин)},$ $9 = 15 \text{ мин}$	4 мин.	0=10 сек (для теста)

Функция	Команда	Опции	Завод. установка	Примечания
Функции PGX	23x	0 — общая поставка (ABC) = PG вкл.	7 вкл/выкл (*80/*81)	х в системе с разделами 0 — трев. А = PG вкл. 1 — трев. В = PG вкл.
Функции PGY	24x	1 — любой раздел на охране = PG вкл. 2 — АВ на охране (не С) = PG вкл. 3 — Пожарная тревога = PG вкл 4 — Тревога Паника = PG вкл. 5 — Любая тревога = PG вкл. 6 — Сбой АС = PG вкл. 7 — PG вкл./выкл. (*80 /*81 для PGX и *90/*91 для PGY) 8 — Один 2 сек. импульс (кнопки *8 = X, *9 = Y)	1 Любой раздел на охране	2 — задержка входа А = PG вкл. 3 — задержка входа В = PG вкл. 4 — А охрана = X вкл, В охрана = Y вкл. 5 — А паника = X вкл, В паника = Y вкл. 6 — Пожар = X вкл, Сбой АС = Y вкл. 7 — PG вкл./выкл. (*80 /*81 для PGX и *90/*91 для PGY) 8 — один 2 сек. импульс (кнопки *8=X, *9=Y)

Функция	Команда	Опции	Завод. установка	Примечания
Контроль радиосвязи	27x	x = 1 — ДА 0 — НЕТ	НЕТ	
Сброс разрешен	28x	1 = ДА 0 = НЕТ	ДА	
Измерение уровня сигнала	298	Команда включает измерение	Кнопки стрелок изменяют адрес, # отключает режим измерения.	
Регистрация контрольной панели в беспроводных модулях релейных выходов	299	Регистрация осуществляется по вводу команды.		
Постановка на охрану без кода доступа	30x	1 = ДА 0 = НЕТ	ДА	Кнопками: А, В, АВС, *1, *2, *3, *4
Индикация сработавших извещателей текстом на дисплее пульта	31x	1 = ДА 0 = НЕТ	ДА	Индикация открытых окон и дверей. Для подробностей нажать ?

Функция	Команда	Опции	Завод. установка	Примечания
<p>Подтверждение охранной тревоги. Срабатывание охранного извещателя в разделе, поставленном на охрану, только записывается в память как неподтвержденная тревога. Тревога включается, если в течение 40 минут срабатывает любой другой охранный извещатель. Если первый извещатель имеет задержку, и тревога не подтверждается другим извещателем, по истечении задержки на вход тревога не включается.</p>	32х	1 = ДА 0 = НЕТ	НЕТ	Тревога подтверждается любым извещателем любого раздела, поставленного на охрану.

Функция	Команда	Опции	Завод. установка	Примечания
Извещатели входной двери. Если функция включена, задержки на вход и выход считаются по 30 сек. Срабатывание датчика входной двери увеличивает задержку на вход, восстановление датчика входной двери прекращает задержку на выход	65х	0 = нет, 1 = извещатели 01–05, 2 = извещатели 46–50	х = 0	Если извещателей входной двери несколько, сработка считается по любому из них, восстановление — если все восстановлены.
Частичная постановка или разбиение на разделы	66х	0 = не разбитая система 1 = частичная постановка (А, АВ, АВС) 2 = разбитая система А, В и общий раздел С (постановка при постановке обоих А и В)	Не разбита	

Функция	Команда	Опции	Завод. установка	Примечания
Индикация сигнала темпера. Индикация темпера при увеличении количества сработавших температурных контактов устройств	681x	1 = реагировать только на новые срабатывания температур. 0 = реагировать на все срабатывания температур.	X = 0	Исключение индикации постоянно нарушенных температурных контактов
Управление PG выходами командами *8 и *9	682x	6821 = ДА. 6820 = НЕТ	ДА	Если ДА, стрелками можно управлять PGX
Индикация тревог в системе на охране	683x	6831 = ДА. 6830 = НЕТ	НЕТ	Запрет отключения дисплея через 3 мин
Постановка на охрану кодом установщика	692x	6921 = ДА. 6920 = НЕТ	НЕТ	Только с разрешения владельца мастер кода
Повышенная чувствительность приемника Увеличение дальности связи в отсутствии помех	694x	0 = норма. 1 = высокая	норма	

Функция	Команда	Опции	Завод. установка	Примечания
Доступ по карте и коду	695x	1 = Код + Карта 0 = Код или Карта	Код или карта	
<p>Реакции устройств и назначение разделам (извещатели, брелки, входы панели и пульта)</p> <p>Оригинальная реакция брелков:</p> <p>Ⓢ (или ●) = Постановка, Ⓞ (или ○) = снятие, одновременное нажатие = Panic.</p> <p>Для частичной постановки, пара кнопок брелков назначается разделам:</p>	61 nn r s (62 nn r s — для кодов и карт)	<p>nn = адрес 01–50</p> <p>r = реакция</p> <p>0 = отключен (включая темпер)</p> <p>1 = оригинальная — означает:</p> <p>для кодов (карт) =</p> <p>Постановка/снятие</p> <p>2 = Паника</p> <p>3 = Пожар</p> <p>4 = 24 часа</p> <p>5 = Прохода</p> <p>6 = Мгновенная</p> <p>7 = Постановка</p> <p>8 = Управление PG (s: 1 = PGX, 2 = PGY, 3 = PGX+PGY)</p>	Оригин. реакция, раздел С	

<p>Раздел А: Ⓜ (или ●) = Пост. А, Ⓜ (или ○) = Пост. АВ</p> <p>Раздел В: Ⓜ (или ●) = Пост. А, Ⓜ (или ○) = Пост. АВ</p> <p>Раздел С: Ⓜ (или ●) = Пост. АВС, Ⓜ (или ○) = Снятие АВС</p> <p>В системе, разбитой на разделы, пара кнопок брелока назначается разделам: А = Постановка/ Снятие А, В = Постановка/ Снятие В, С = Постановка/ Снятие АВС</p>		<p>9 Постановка/ Снятие (перекл.) s = Раздел 1 = А, 2 = В, 3 = С — нужно вводить даже, если система не разбита на разделы.</p>		
--	--	---	--	--

Функция	Команда	Опции	Завод. установка	Примечания
Расписание автоматической Постановки/ Снятия	64nahlmm	n — номер расписания (0–9) a — действие: 0 = нет 1 = Постановка ABC 2 = Снятие ABC 3 = Постановка A 4 = Постановка B 5 = Снятие A 6 = Снятие B hh — часы, mm — минуты	Нет	Расписания действительны для каждого дня
Изменение кода установщика	5 NC NC	NC = новый код	8080	Введите NC дважды
Вход в режим пользователя	292	Переход в режим пользователя	—	

Программирование кодов доступа и карт осуществляется с пульта управления или с помощью программного обеспечения OLink при подключении к компьютеру. В табл. 3.3 представлены команды для изменения кода установщика, мастер-кода и добавления кодов или карт пользователей.

Таблица 3.3

Программирование кодов доступа (карт)

Название кода	Команда	Примечания
Установщика	5 NC NC	<p>Программируется только в режиме настроек.</p> <p>NC = новый код (вводится дважды) — карта не используется.</p> <p>Заводская установка: 8080.</p> <p>Код можно менять, но нельзя удалить.</p> <p><i>Пример ввода: 5 4567 4567</i></p>
Мастер	*5 MC NC NC	<p>Программируется при снятии системы с охраны.</p> <p>MC = мастер код или карта (заводская установка 1234).</p> <p>NC = новый код или карта — код вводится дважды, карта подносится один раз.</p> <p>Используется или код или карта (и карта и код невозможны).</p> <p>Мастер код можно менять, но не удалять (для упрощения пользования системой можно использовать Мастер карту, вместо Мастер кода).</p> <p>Реакция мастер кода: постановка/снятие для всех разделов.</p>

Название кода	Команда	Примечания
		<p>Сброс Мастер-кода на заводскую установку 1234 — в режиме настроек набрать 291 (сброс только Мастер кода).</p> <p><i>Пример создания мастер-карты:</i> *5 1234 и предъявить карту считывателю пульта.</p> <p><i>Пример создания мастер-кода:</i> *5 1234 7654 7654.</p>
Пользователя	*6 MC nn NC	<p>Программируется при снятии системы с охраны.</p> <p>MC = Мастер код или Мастер карта. nn = номер пользователя 01–50. NC = новый код или карта.</p> <p>Заводская установка: нет кодов и карт пользователей.</p> <p>Каждый пользователь может иметь и код и карту, при этом команда выполняется дважды — сначала для кода, затем для карты или наоборот.</p> <p>Каждый код/карта могут иметь индивидуальную реакцию, запрограммированную установщиком в режиме настроек. В разбитой на разделы системе, коды/карты могут назначаться различным разделам.</p> <p><i>Пример установки для пользователя 12 кода 9087:</i> *6 1234 12 9087</p>

Как было описано ранее, *рабочий (пользовательский) режим* предназначен для ежедневной работы с системой пользователей при постановке на охрану, снятии с охраны, управлении автоматикой и пр.

Командные функции, доступные для пользователя и начинающиеся со * следующие:

- *1 — постановка всей системы (аналог кнопки ABC);
- *2 — постановка раздела А (аналог кнопки А);
- *3 — постановка А и В, или только В (аналог кнопки В);
- *4 — просмотр памяти событий;
- *5 — новый Мастер код/карта;
- *6 — программирование кодов/карт;
- *7 — работа под принуждением (вводится перед кодом доступа, для передачи сообщения о принуждении);
- *8 — управление первым релейным выходом;
- *9 — управление вторым релейным выходом;
- *0 — Вход в режим настроек или для входа в режим пользователя.

Режим настроек предназначен только для установщика, использующего код установщика, и используется для регистрации беспроводных устройств, программирования параметров системы и пр.

Режим обслуживания предназначен для администратора, использующего мастер код для осуществления частичное программирования системы, например, при программировании кодов пользователей.

В режиме обслуживания возможно: тестировать устройства (тревог не будет), посмотреть, для каких пользователей запрограммированы карты/коды; исключать устройства (на один цикл постановки на охрану или на все время); устанавливать время для часов; программировать расписание авто постановки/снятия; программировать номера телефонов для сообщений пользователям.

Например, для просмотра пользователей с запрограммированными кодами/картами необходимо выполнить следующие действия:

1. Контрольная панель должна быть в режиме пользователя — если нет, введите *0 *Мастер код или карта* (заводская установка: 1234), причем контрольная панель должна быть снята с охраны;

2. Нажать **5**, после чего на дисплее будут отображены «Codes 01: Code»);

3. Используя кнопки со стрелками, пролистать все коды (01–50), символ **A** показывает запрограммирован ли код, символ **B** показывает запрограммирована ли карта.

4. Для выхода из режима просмотра нажать кнопку **#**.

5. Для выхода из режима пользователя нажать кнопку **#**.

3.3. Экспериментальное задание

1. Вскрыть крышку контрольной панели, разобраться с подключениями на клеммой колодке, подключить к контрольной панели пульт управления (клавиатуру) с помощью RJ кабеля, подключить питание, если проводной пульт подключен, он будет показывать режим настройки, если нет, контрольную панель следует сбросить в заводские установки, закрыть крышку корпуса.

2. Поочередно зарегистрировать беспроводные брелок и сирену (см. раздел регистрации беспроводных устройств).

3. Подключить источники питания к беспроводному извещателю и зарегистрировать его в системе.

4. Измерить уровень сигнала от беспроводных устройств, удаляя их на различные расстояния от приемно-контрольной панели (см. раздел измерения уровня сигнала).

5. Выполнить программирование контрольной панели с пульта, ознакомившись с функциями: Вход в режим регистрации, установки Времени задержки на выход, а вход и Длительности тревоги, Частичная постановка или разбиение на разделы, Реакции устройств и назначение разделам, Установка встроенных часов, Расписание автоматической Постановки/Снятия, Вход в режим пользователя, Редактирование текстов пультов.

6. Ознакомиться с органами индикации и управления пульта, запрограммировать коды доступа и карты пользователей для членов бригады.

7. Ознакомиться с режимом обслуживания, просмотреть список пользователей с запрограммированными кодами и картами.

8. Ознакомиться с рабочим режимом пользователя, и поставить/снять с охраны систему.

8. Ознакомиться с программированием и управлением системой охраны с помощью ПК через ПО OLink, подключив к компьютеру контрольную панель с использованием интерфейсного кабеля.

3.4. Контрольные вопросы

1. Перечислить основные характеристики беспроводной системы охраны Oasis.

2. Какое оборудование входит в состав системы?

3. Перечислить порядок подключения устройств в системе охраны.

4. Какова архитектура контрольной панели системы?

5. Назвать основные функции контрольной панели и ее режимы работы.

6. Особенности работы контрольной панели с проводными устройствами.

7. Что необходимо выполнить перед первым включением контрольной панели и конфигурированием системы охраны?

8. Порядок регистрации беспроводных устройств в системе.

9. Как выполнить программирование контрольной панели и основные используемые функции и команды.

10. Для чего и как устанавливается задержка на выход/вход?

11. Разбиение системы на разделы, особенности постановки/снятия разбитой на разделы системы.

12. Охарактеризовать режимы настроек, обслуживания и пользователя системы охраны.

13. Основные функции пульта управления, порядок программирования кодов и карт доступа пользователей.

4. ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ИНТЕГРИРОВАННОЙ СИСТЕМЫ ОХРАНЫ «ОРИОН»

4.1. Цель

Ознакомиться с составом оборудования системы охранной сигнализации и изучить возможности конфигурирования системы

4.2. Краткие теоретические сведения

Общее описание комплексной системы безопасности (КСБ) «Орион» характеризует систему как объектно-ориентированную, предназначенную для организации рабочего места дежурного оператора службы охраны и управления работой следующих подсистем: охранной и пожарной сигнализации, контроля доступа, видеонаблюдения, управления пожарной автоматикой, управления инженерными подсистемами [16]. Система «Орион» обеспечивает сбор, обработку, передачу, отображение и регистрацию извещений о состоянии объектов системы.

Модульная структура системы, основанная на древовидной сетевой архитектуре, позволяет оптимально оборудовать как малые, так и большие распределенные объекты, а защищенный протокол обмена данными по каналу связи между приборами обеспечивает достоверную передачу сигналов тревоги. Основным аппаратным интерфейсом системы является RS-485, обеспечивающий через двухпроводную магистраль связь всех приемно-контрольных приборов и сетевых контроллеров системы через каналобразующее оборудование с автоматизированным рабочим местом (АРМ) на базе ПК. Основные технические характеристики локальной интегрированной системы «Орион» приведены в табл. 4.1.

Основные технические данные локальной ИСО «Орион»

Параметр	Значение
Количество приборов, подключаемых к линии интерфейса RS-485	до 127
Количество зон, объединяемых в разделы (АРМ «Орион Про»)	до 16 000
Количество зон, объединяемых в разделы (ПКУ «С2000М»)	до 2048
Количество разделов (АРМ «Орион Про»)	до 10 000
Количество разделов (ПКУ «С2000М»)	до 512
Количество точек доступа	до 254
Количество выходов для управления внешними устройствами (АРМ «Орион Про»)	до 16 000
Количество выходов для управления внешними устройствами (ПКУ «С2000М»)	до 255
Количество пользователей (АРМ «Орион Про»)	не ограничено
Количество пользователей (ПКУ «С2000М»)	до 2047
Длина линии интерфейса RS-485 (без использования дополнительных повторителей)	до 3 000

Состав основного оборудования интегрированной системы охраны (ИСО) Орион подразделяется на такие основные группы устройств, как сетевые контроллеры, преобразователи интерфейсов, приемно-контрольные приборы, контроллеры доступа и считыватели, клавиатуры, блоки индикации и управления, адресные системы ОПС и противопожарной автоматики, релейные блоки, источники бесперебойного питания, устройства речевого оповещения и передачи извещений [16].

Основным сетевым контроллером является С2000М — пульт контроля и управления охранно-пожарный, предназначенный для работы в составе адресной системы охранно-пожарной сигнализации и управления противопожарным оборудованием, обеспечивающий связь с другими приборами системы по проводной линии связи RS-485 на расстоянии до 3 км.

В группу преобразователей интерфейсов входят следующие каналообразующие устройства [16]:

1. С2000-Ethernet — преобразователь интерфейсов RS-485/RS-232 в Ethernet, предназначенный для организации связи приборов по локальной сети с целью получения показаний приборов учета с удаленных объектов.

2. С2000-РПИ — радиоповторитель интерфейсов, предназначенный для трансляции данных интерфейса RS-232/RS-485 по радиоканалу с целью формирования между двумя или более радиоповторителями в диапазоне частот 2400...2483,5 МГц на расстоянии до 600 м моста между различными сегментами сети интерфейса RS-485 с сетевой топологией «точка — точка» или «звезда».

3. С2000-ПИ — преобразователь интерфейсов RS-232/RS-485, повторитель интерфейса RS-485 с гальванической развязкой, предназначенный для гальванической изоляции и взаимного преобразования сигналов интерфейса RS-232 и сигналов двухпроводного магистрального интерфейса RS-485 с целью подключения приборов к ПК с АРМ «Орион Про» или АРМ «С2000» или для увеличения длины двухпроводного магистрального интерфейса RS-485.

4. ПИ-ГР — преобразователь интерфейсов с гальванической развязкой, предназначенный для гальванической изоляции и взаимного преобразования сигналов интерфейса RS-232 и сигналов двухпроводного магистрального интерфейса RS-485 с целью подключения приборов к ПК с АРМ «Орион Про» или АРМ «С2000».

5. C2000-USB — преобразования сигналов интерфейса USB в сигналы двухпроводного магистрального интерфейса RS-485, предназначенный для подключения приборов к ПК с АРМ «Орион Про» или АРМ «С2000».

6. USB-RS232 — преобразователь интерфейсов USB-RS232, предназначенный для гальванической изоляции и взаимного преобразования сигналов интерфейса USB и сигналов последовательного интерфейса RS-232, с целью подключения ПК к пульту «С2000М» при его программировании.

7. RS232-TTL — преобразователь интерфейсов, предназначенный для преобразования сигналов интерфейса RS-232 в сигналы последовательного интерфейса с уровнями 5В TTL/CMOS с целью подключения радиопередатчика АТС100 радиосистемы передачи извещений LARS или радиопередатчика TRX-150 радиосистемы «Орион Радио» к пульту «С2000М» для радиомониторинга охраняемых объектов.

8. Ethernet-FX (Ethernet-FX-MM, Ethernet-FX-SM40, Ethernet-FX-SM40SA, Ethernet-FX-SM40SB) — преобразователи волоконно-оптические, предназначенные для преобразования сигналов интерфейса Ethernet стандартов 10/100Base-T(X) в оптические сигналы стандартов 100Base-FX, либо 100Base-FX WDM с целью обмена данными между охранно-пожарными приборами на расстояние до 40 км по одномодовым или многомодовым оптическим кабелям.

9. Ethernet-SW8 — неуправляемый коммутатор для разветвления сетей Ethernet стандартов 10/100Base-T(X), предназначенный совместно с преобразователями интерфейсов «С2000-Ethernet» коммутировать сигналы охранно-пожарных приборов ИСО «Орион».

Группа приемно-контрольных приборов представлена следующими устройствами, различающихся по числу шлейфов сигнализации и наличием выхода для управления считывателями для системы контроля доступом [16]:

1. Сигнал-20, Сигнал-20М — приборы приемно-контрольные охранно-пожарные, предназначенные для использования в автономном режиме или в составе ИСО «Орион» для контроля различных ти-

пов охранных и пожарных неадресных извещателей с нормально-замкнутыми или нормально-разомкнутыми контактами и релейного управления внешними исполнительными устройствами [17].

2. Сигнал-20П — блок приемно-контрольный охранно-пожарный, способный выполнять функцию адресного расширителя шлейфов, имеет также выход управления считывателем карт или ключей touch-memory.

3. Сигнал-10, С2000-4 — приборы приемно-контрольные охранно-пожарные с функцией управления считывателями [18].

Группа контроллеров доступа и считывателей представлена устройствами:

1. С2000-2 — контроллер доступа, предназначенный для управления доступом через одну или две точки прохода с использованием двух считывателей, возможностью управления двум замками и с двумя шлейфами охранной сигнализации для подключения дверных извещателей.

2. С2000-BIOAccess-F18, С2000-BIOAccess-MA300 — биометрические контроллеры доступа, обеспечивающие считывание отпечатков пальцев, карт доступа, а первая модификация обеспечивает ввод PIN-кода со встроенной клавиатуры, при этом оба контроллера работают как в режиме контроллера, так и считывателя и имеют сетевой Ethernet (TCP/IP)-интерфейс.

3. Proxy-5MSG, Proxy-5MSB, Proxy-5MS-USB, Proxy-KeyAV, Proxy-KeyAH, Proxy-KeyMV, Proxy-KeyMH, С2000-Proxy и пр. — считыватели бесконтактные различных модификаций.

В группе адресных систем кроме базовых адресных ОПС и противопожарной автоматики линейка оборудования компании Болид содержит оборудование адресной подсистемы на основе «С2000-Периметр», адресной радиоканальной подсистемы на основе «С2000Р-APP32».

Приборы речевого оповещения представлены таким оборудованием, как информатор телефонный С2000-ИТ, устройство оконечное системы передачи извещений по каналам сотовой связи GSM УО-

4С, устройство оконечное объективное системы передачи извещений по телефонным линиям, сетям GSM, Ethernet C2000-PGE.

С характеристиками и принципом функционирования перечисленных устройств и устройств других групп можно ознакомиться их технической документации компании Болид.

Для знакомства с принципом построения и конфигурирования комплексной системой безопасности объектов ОРИОН, включающей в себя подсистемы охранно-пожарной сигнализации (ОПС) и контроля и управления доступом (СКУД), рассмотрим упрощенную обобщенную структуру, приведенную на рис. 4.1, которая используется в лабораторных целях и демонстрирует возможности системы ОРИОН, имеющей сетевую структуру и реализована на приемно-контрольном приборе охранно-пожарном (ПКП) Сигнал-20SMD (20 шлейфов, 5 выходов); для охранно-пожарной подсистемы сигнализации, на сетевом ПКП С2000-4 (4 шлейфа, 2 реле, контроллер TouchMemory) — для подсистемы СКУД, при общем управлении на базе контроллера С2000 (пульт контроля и управления для конфигурирования системы, постановки/снятия с охраны разделов, отображения прошедших событий и управления контролем доступа), либо с помощью АРМ «ОРИОН», установленном на персональном компьютере.

Подключение приборов к ПЭВМ осуществляется через СОМ-порт и преобразователь интерфейсов с гальванической развязкой (ПИ-ГР). Кроме того дополнительные требуемые приборы для ИСО следующие: С2000-БИ — блок индикации, служащий для индикации состояния до 60 разделов; С2000-Прогу — считыватель карт доступа; пассивный инфракрасный извещатель; магнитоконтактный дверной извещатель; тепловой пожарный извещатель, дымовой пожарный извещатель; тревожная кнопка; световой оповещатель.

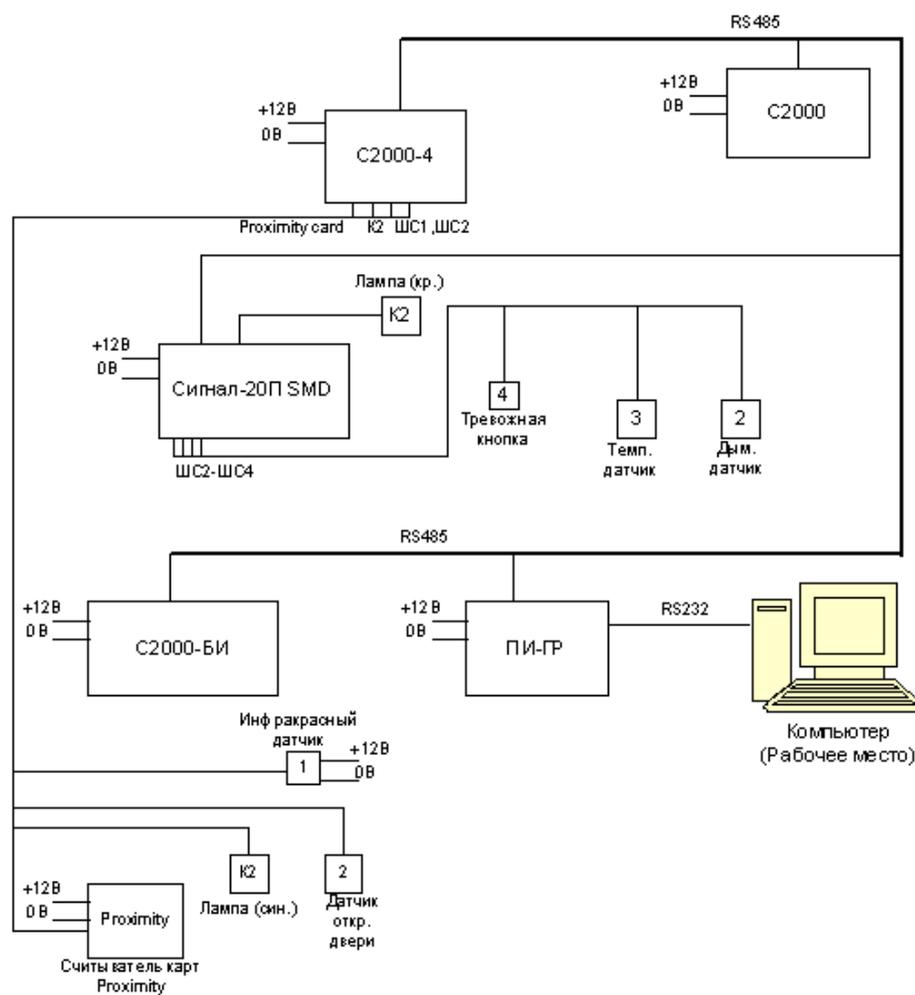


Рис. 4.1. Обобщенная структурная схема системы ОРИОН лабораторного эксперимента

Функции видеоконтроля в АРМ «Орион» могут осуществляться установкой на компьютер видеоподсистемы наблюдения Инспектор+ с многоканальной платой оцифровки видео, взаимодействующей с АРМ Орион.

Для подключения приборов к интерфейсу RS-485 служат контакты «А» и «В» в каждом из сетевых устройств системы. Интерфейс RS-485 предполагает использование соединения между приборами типа «шина», согласованной с двух сторон согласующими резисторами сопротивлением 620 Ом, которые устанавливаются на первом и последнем приборах в линии, как показано на рис. 4.2. В приемно-контрольных приборах согласующее сопротивление присутствует на плате и может быть включено в линию установкой перемычки.

Ответвления на линии нежелательны, так как они увеличивают отраженный сигнал в линии, но при необходимости допустимы, и при этом согласующий резистор на отдельных ответвлениях не устанавливается.

Сопротивление каждой линии интерфейса (А или В) от пульта до наиболее удаленного прибора должно быть не более 200 Ом. При наличии сильных внешних электромагнитных полей рекомендуется использовать экранированную витую пару проводов. Преобразователь интерфейсов должен быть подключен к собственному источнику питания.

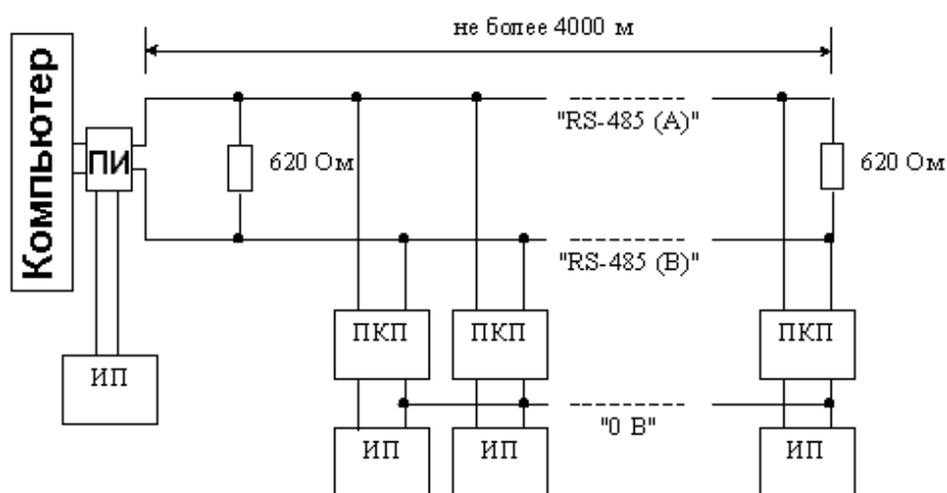


Рис. 4.2. Схема последовательного подключения приборов по RS-485

Для увеличения длины сегмента канала связи используется повторители-ретрансляторы интерфейса RS-485 с автоматическим переключением направления передачи (П), как показано на рис. 4.3. Например, повторитель с гальванической изоляцией I-7510 позволяет увеличить длину линии на 1500 м и обеспечивает гальваническую изоляцию между сегментами линии. Цепи «0 В» изолированных сегментов не объединяются. Также повторители можно использовать для построения конфигурации «звезда», как показано на рис. 4.4.

Каждый подключенный к пульту по интерфейсу RS-485 прибор должен иметь уникальный сетевой адрес, хранящийся в энергонезависимой памяти прибора. Изменение сетевых адресов производится с помощью программы Администратор базы данных либо с использованием пульта контроля и управления С2000.

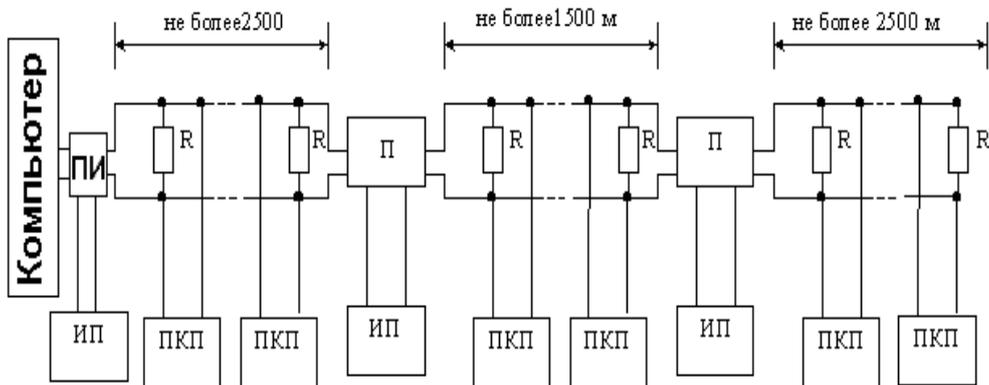


Рис. 4.3. Увеличение длины линии за счет повторителей интерфейса

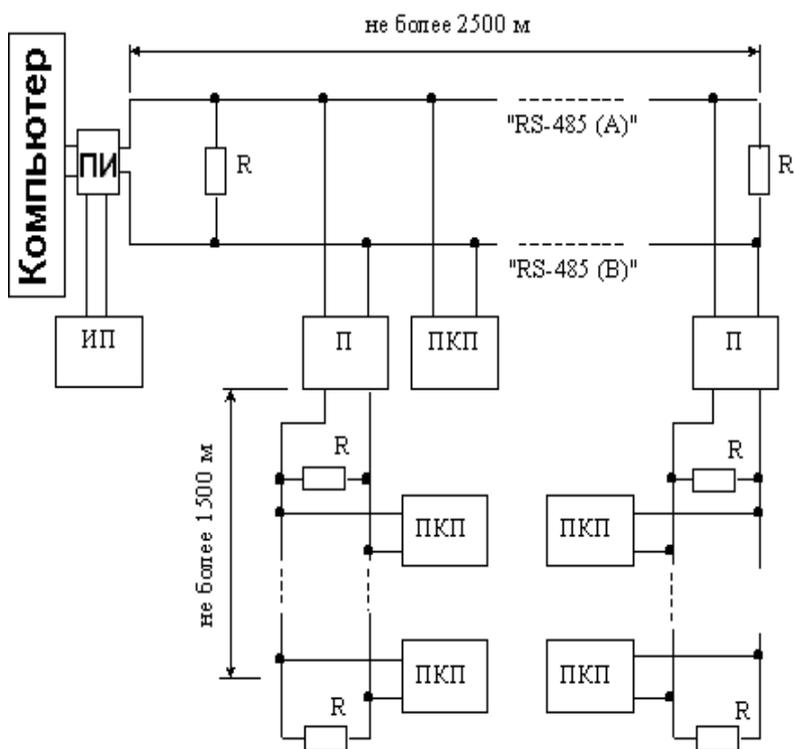


Рис. 4.4. Построение конфигурации «звезда» при помощи повторителей интерфейса

Подключение сетевых устройств производится при снятой верхней крышке прибора на его клеммной колодке согласно приводимой в технической документации схеме подключения [17, 18]. Так схема подключения блока контроля и управления С2000 показан на рис. 4.5, схема подключения ПКП Сигнал20SMD — на рис. 4.6, а схема подключения контроллера подсистемы управления доступом С2000-4 представлена на рис. 4.7.

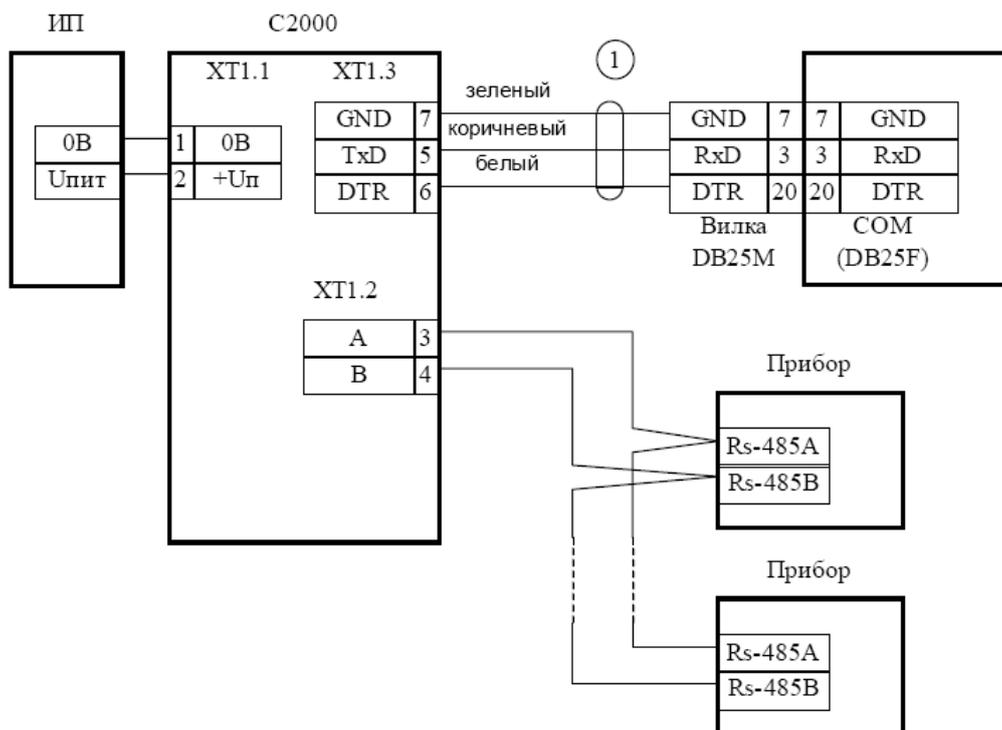


Рис. 4.5. Схема подключения пульта контроля и управления С2000

Конфигурирование КСБ Орион осуществляется как на аппаратном уровне при поочередном подключении устройств системы и использовании команд, вводимых с клавиатуры пульта контроля и управления С2000, так и на программном уровне с использованием программного обеспечения ИСО ОРИОН, установленном на компьютере.

При аппаратном конфигурировании следует подключить один из приборов к общей шине пульта контроля и управления, на ЖКИ которого появится сообщение о найденном приборе. После этого необходимо изменить его адрес, выполнив последовательно следующие действия:

- войти в меню программирования нажатием на пульте контроля и управления клавиши PROG;
- ввести пароль установщика;
- выбрать пункт меню «Адреса»;
- выбрать пункт меню «Адресный прибор»;
- набрать адрес прибора, который необходимо изменить;
- набрать новый адрес прибора.

После того как С2000 обнаружил прибор, нужно настроить его конфигурацию согласно следующей последовательности действий:

- войти в меню программирования нажатием на пульте контроля и управления клавиши PROG;
- ввести пароль установщика;
- выбрать пункт меню «Конфигурации»;
- выбрать пункт меню «Изменение»;
- набрать адрес конфигурируемого прибора.

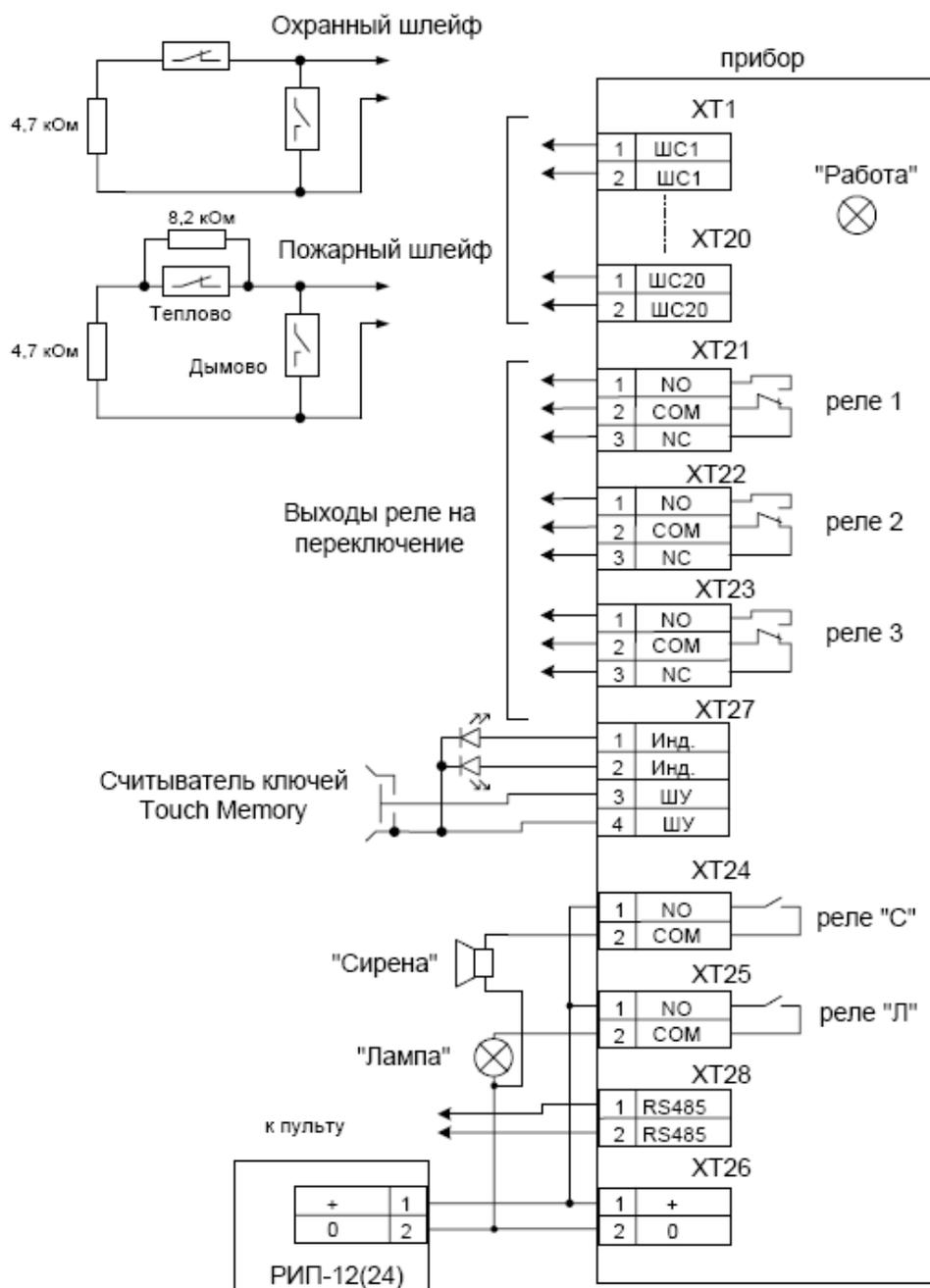


Рис. 4.6. Схема подключения ПКП Сигнал 20SMD

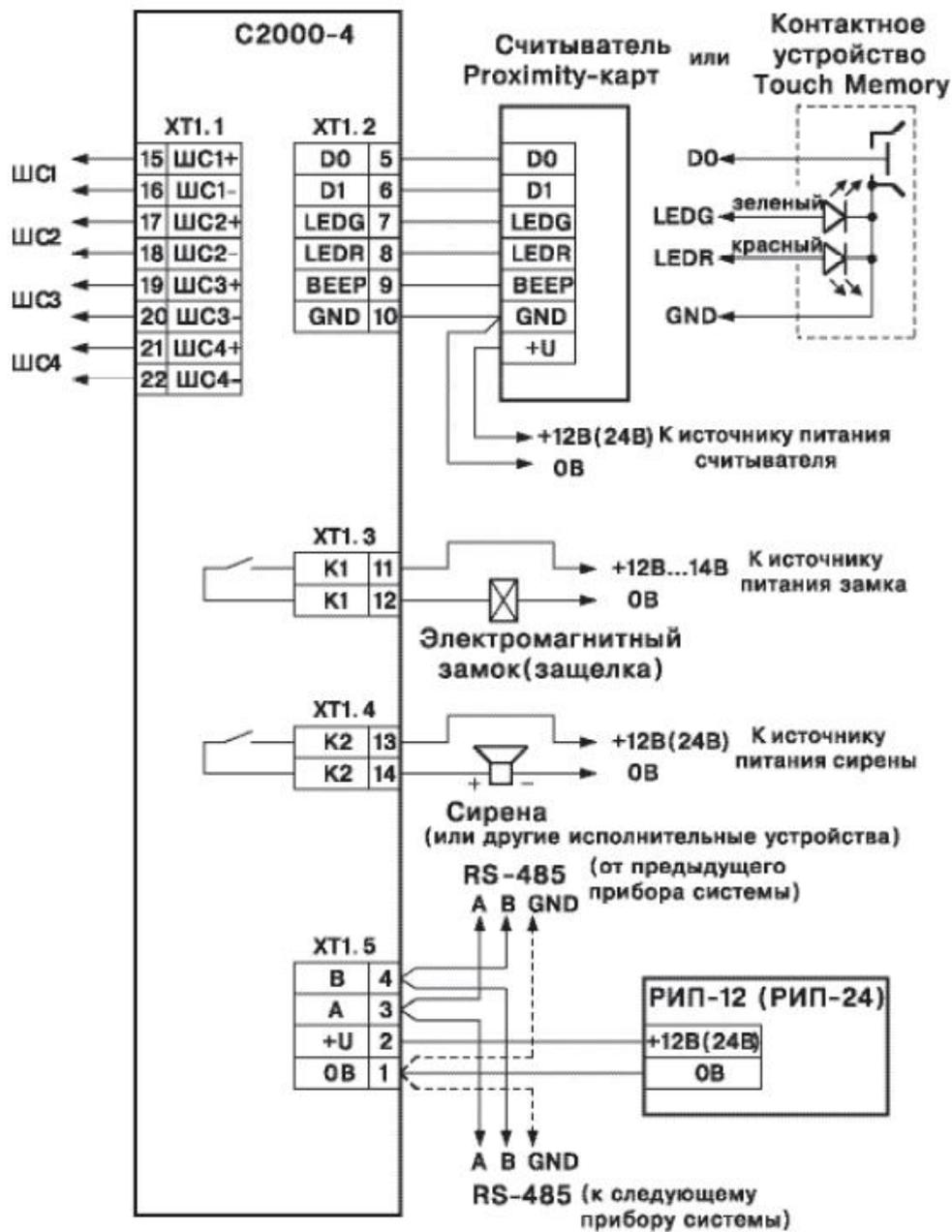


Рис. 4.7. Схема подключения контроллера подсистемы управления доступом С2000-4

В конфигурации прибора надо изменить «Тип шлейфа» для подключенных ШС, так же надо настроить привязку реле к ШС. Тип ШС может быть пожарный, охранный, технологический и пр. и выбирается при детальном ознакомлении с технической документацией к прибору.

После проделанных операций, можно приступить к использованию извещателя, подключенного к ШС прибора. Например, чтобы взять на охрану ШС необходимо выполнить следующее:

- нажать клавишу PROG;
- ввести пароль установщика;
- выбрать пункт меню «Взятие»;
- выбрать пункт меню «Взятие ШС»;
- набрать адрес прибора;
- набрать номер ШС.

Если в момент взятия ШС он находится в режиме тревоги или не готов к использованию, то ШС не возьмётся на охрану. Для снятия с охраны ШС необходимо выполнить последовательность операций:

- нажать клавишу PROG;
- ввести пароль установщика;
- выбрать пункт меню «Снятие»;
- выбрать пункт меню «Снятие ШС»;
- набрать адрес прибора;
- набрать номер ШС.

Подобным образом производится конфигурирование каждого прибора, по отдельности подключаемого к пульту С2000:

Программное конфигурирование системы «Орион» предварительно требует ознакомления с составом его утилит или программ-подсистем [19], таких как:

- Оперативная задача (orion.exe), предназначенная для ведения журнала событий, управления взятием на охрану и снятием с охраны объектов, контроля и графического отображения состояния разделов и зон, речевого оповещения при возникновении тревог;

- Администратор базы данных (abd.exe), предназначенный для управления вводом, редактированием, обменом данными, необходимыми для правильного функционирования системы охраны;

- Генератор отчетов (report.exe), служащий для формирования отчетов о состоянии и событиях аппаратной ИСО в определяемый пользователем интервал времени;
- Мастер системы (master.exe), предназначенный для архивирования, реставрации, удаления информации базы данных системы;
- Мастер конфигурации приборов (uprog.exe), выполняющий функции настройки конфигурационных параметров приборов;
- Мастер шлейфов (shleifes.exe), служащий для контроля и отображения состояния шлейфов в реальном времени;
- Редактор планов, позволяющий создать графическое изображение планов помещений объектов охраны;
- Демонстратор (demon.exe), предназначенный для эмуляции работы приборов, занесенных в базу данных системы;
- Отчет о находящихся на объекте (Last rpt.exe), выводящий список находящихся на объекте сотрудников или посетителей по результатам анализа журнала событий;
- Локальный и сетевой «Учет рабочего времени» (wt.exe и NWTime.exe), позволяющий формировать отчеты по учету рабочего времени сотрудников.

После того как все приборы подключены к пульту управления С2000, который в свою очередь, подключен через ПИ-ГР к ПК, а также установлено ПО АРМ «ОРИОН» [19], для настройки АРМ «Орион» общий порядок действий определяется следующими этапами:

1. Перевести пульт С2000 в «Режим программирования».
2. Запустить утилиту «UPROG».
3. Произвести поиск подключенных приборов.
4. Выбрать нужный прибор и изменить его конфигурацию согласно инструкции (адрес, тип шлейфа, управление реле).
5. Записать изменённую конфигурацию в прибор.
6. Запустить утилиту «Редактор планов».
7. Выбрать габариты плана помещения.
8. Нарисовать план помещения.

9. Сохранить план помещения.
10. Запустить программу «Администратор базы данных (АБД)».
11. Произвести опрос подключенных приборов.
12. Добавить план помещения.
13. С помощью «Редактора разделов» добавить на план помещения используемые приборы и извещатели.
14. Создать базу данных и занести в неё информацию о физической и логической структуре системы (приборы, ШС, реле, разделы).
15. Добавить сотрудников и назначить им пароли.
16. Обновить БД в «Оперативной Задаче».
17. Записать БД в пульт С2000.
18. Запустить программу «Оперативная задача (ОЗ)», в которой можно ставить или снимать с охраны разделы, просматривать журнал посещений и журнал тревог.

Рассмотрим очередность работы с программным обеспечением системы. Запустив утилиту *конфигурирования приборов uprog* осуществляется поиск подключенных к компьютеру приборов системы, как показано на рис. 4.8.

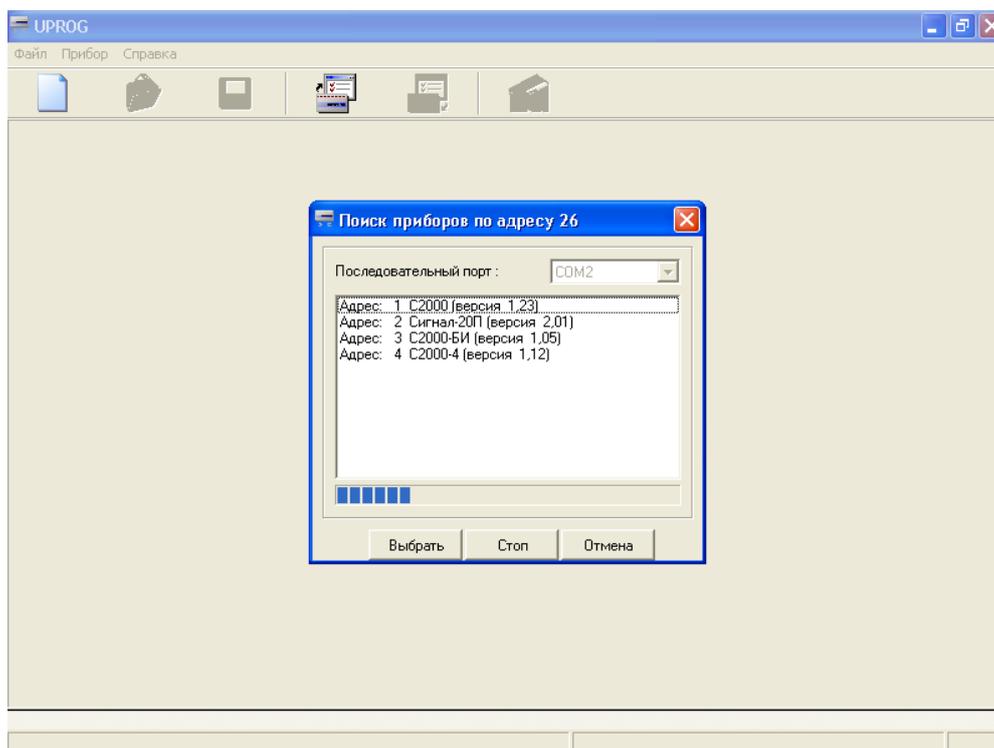


Рис. 4.8. Поиск подключенных приборов системы «Орион»

Далее для выбранного прибора необходимо задать адрес, типы задействованных шлейфов сигнализации, управление реле, что иллюстрируется следующими рисунками 4.9–4.11. После чего нужно записать измененную конфигурацию, используя известные команды пунктов меню или кнопки на панели инструментов конфигуратора.

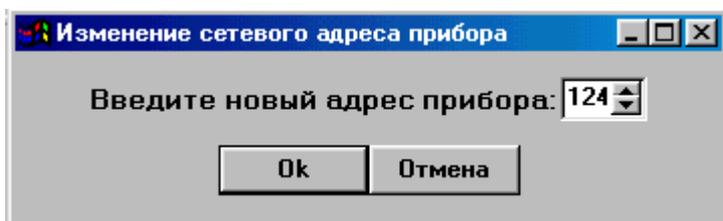


Рис. 4.9. Установка нового сетевого адреса прибора системы

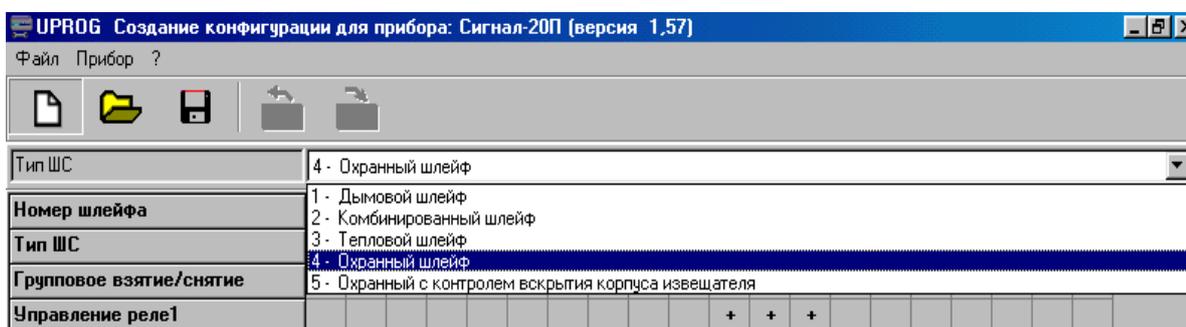


Рис. 4.10. Выбор типа шлейфа сигнализации прибора системы

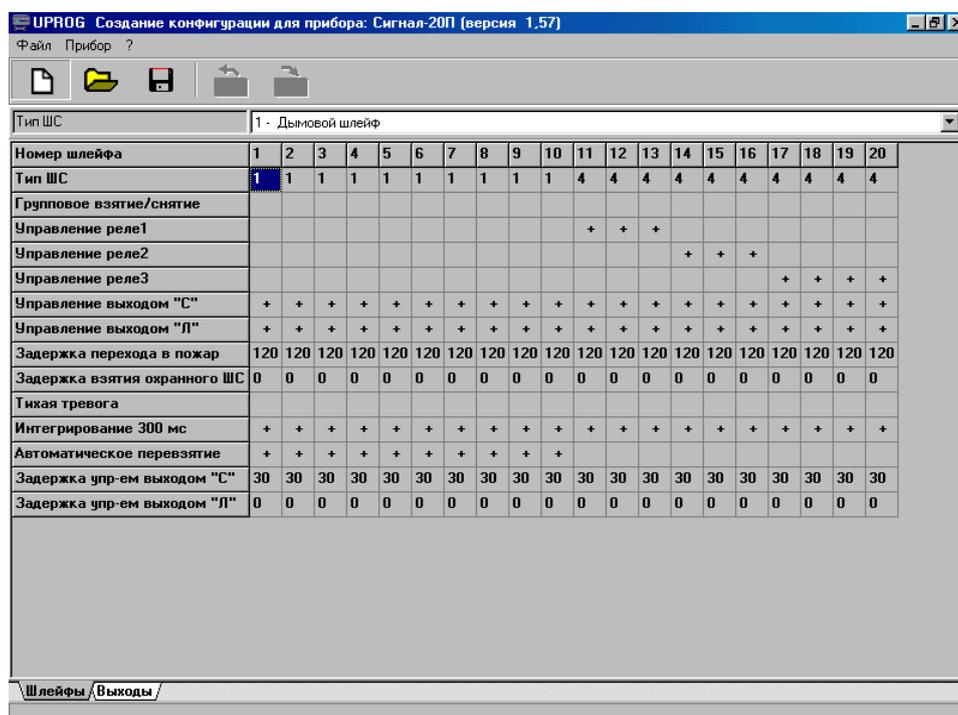


Рис. 4.11. Задание общей конфигурации ПКП Сигнал

План помещения, создаваемый в одном из графических редакторов (в частности можно использовать встроенный редактор планов помещений), необходим на одном из этапов работы с администратором баз данных, начало работы с которым при первом обращении к нему начинается с запуска «Мастера системы», как показано на рис. 4.12, для очистки базы данных и после начала его работы, сопровождающегося запросом пароля на удаление данных (по умолчанию «1»), база данных будет очищена и готова к заполнению.

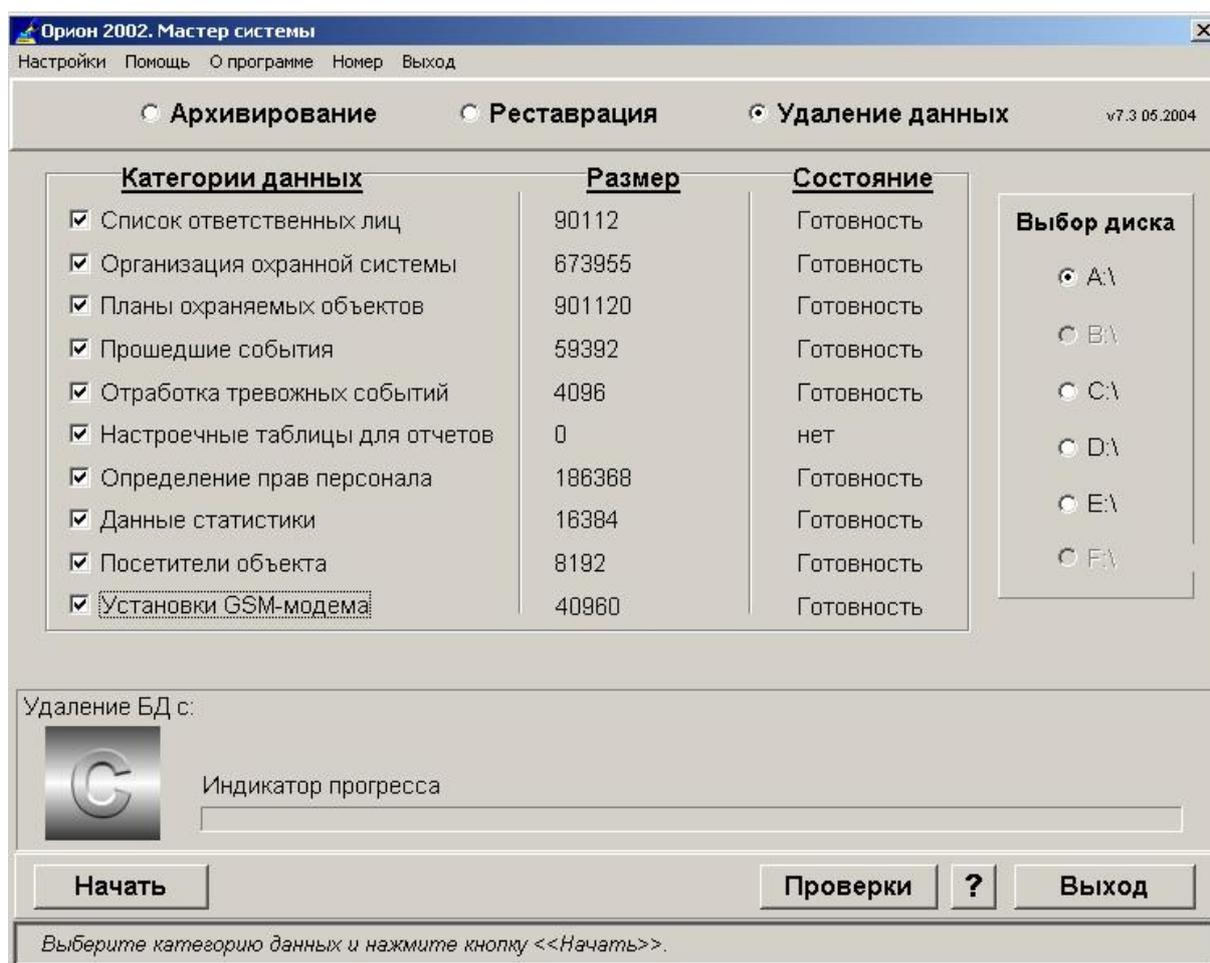


Рис. 4.12. Использование мастера системы

Запустив администратор баз данных на первом этапе необходимо провести чтение конфигурации подключенных приборов, как показано на рис. 4.13.

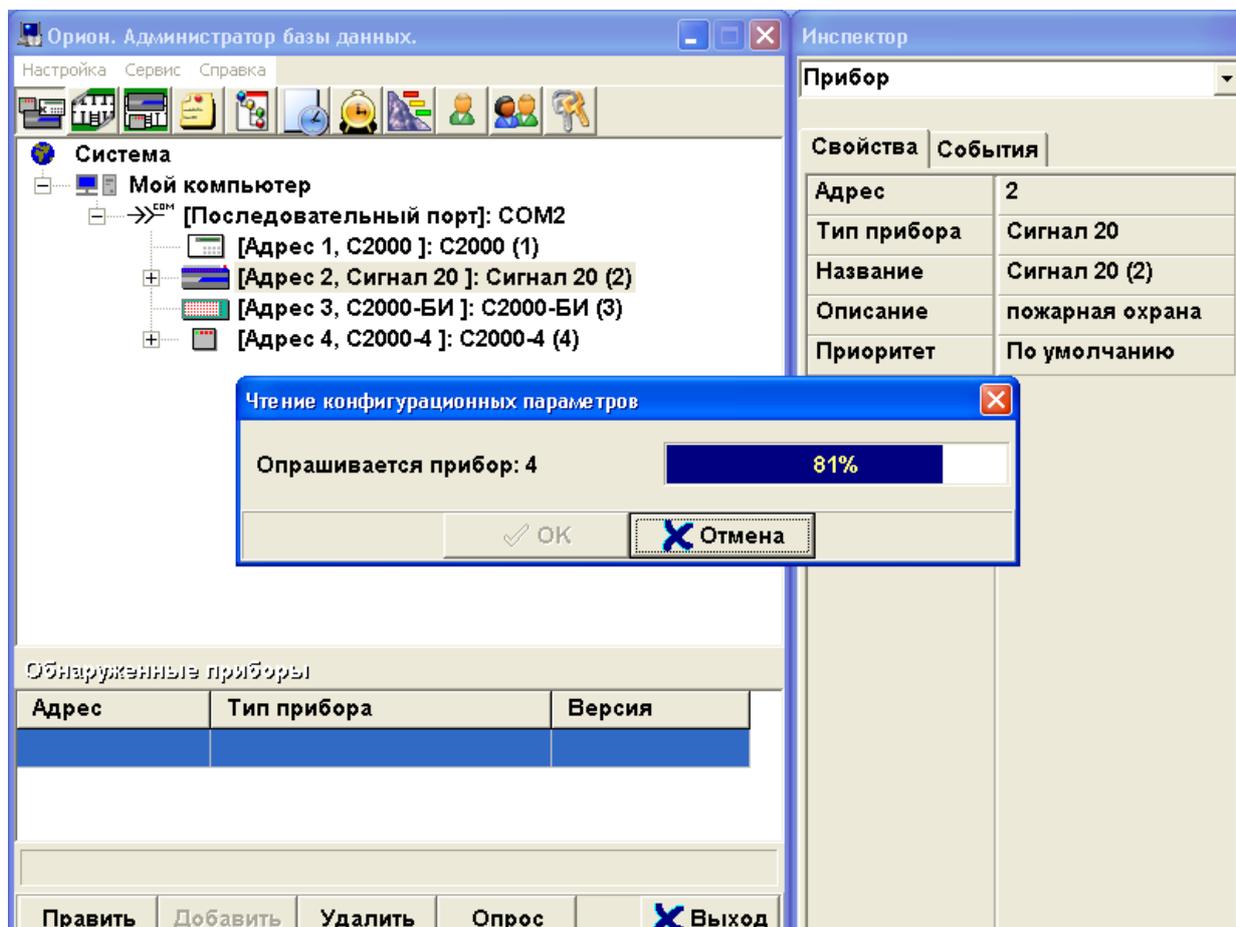
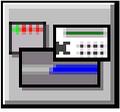
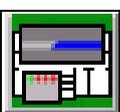


Рис. 4.13. Чтение конфигурации подключенных приборов системы в администраторе баз данных

Все команды для работы в администраторе баз данных доступны в пунктах меню и на панели инструментов, назначение пиктограмм которой приведено в табл. 4.2. Кроме основных кнопок панели инструментов администратор баз данных имеет кнопки для работы со страницами ввода персонала, определения существующих на объекте подразделений, задания паролей для определения прав доступа персонала, формирования окон времени для персонала, создания сценариев управления, задания расписания запусков сценариев управления и формирования дерева управления.

Назначение основных кнопок панели инструментов администратора баз данных

Вид кнопки	Название	Название страницы
	Адреса приборов	Страница адресов приборов
	Планы помещений	Страница планов охраняемых объектов
	Уровни доступа	Страница формирования уровней доступа
	Структура системы	Страница соответствия физической и логической структур охранной структуры

Дополнительное окно «Инспектор» служит для отображения свойств выбранного объекта или событий на данном объекте (приборе, разделе, шлейфе и так далее), переключение на страницу которого происходит по нажатию кнопки «Адреса приборов».

На данной вкладке осуществляется добавление, редактирование и удаление информации с использованием соответствующих кнопок. Добавление информации производится как с помощью стандартной кнопки «Добавить», так и с помощью кнопки «Опрос», а при редактировании информации о приборе при сохранении данных все значения параметров будут записаны в прибор. Для более детального ознакомления о редактируемых параметрах необходимо ознакомиться с соответствующими инструкциями к приборам.

На втором этапе работы с администратором баз данных необходимо ввести графические чертежи-планы охраняемых объектов на странице «Планы помещений», переключение на которую происхо-

дит по нажатию соответствующей кнопки панели инструментов. Как указывалось, ранее предварительно для прорисовки планов помещений охраняемого объекта предназначена программа «Редактор планов», хотя вместо нее можно использовать любой графический редактор, создающий файлы формата BMP.

На третьем этапе после добавления планов охраняемого объекта необходимо выполнить добавление раздела на выбранный план из дерева планов объектов системы, прорисовать области заданного раздела, добавить показатели температуры и задымленности на план помещения, зоны (шлейфы), расставить извещатели, относящиеся к добавляемой зоне. Для прорисовки разделов и для расстановки извещателей выбранной зоны на плане существуют определенные особенности, интуитивно легко понятные, а для детального ознакомления с которыми можно воспользоваться технической документацией к системе. В результате области добавленных разделов и извещатели зон будут показаны на планах и будут выделяться при прохождении над ними курсора. Переход к определенному разделу может происходить по выбору данного раздела на дереве планов или при подведении курсора к области данного раздела на плане и нажатии левой клавиши мыши. Аналогично необходимо добавить остальные элементы охраны и контроля доступа, такие как приборы, считыватели, реле и пр.

Для добавления точек доступа (дверей, турникетов и пр.) объекта в базу данных необходимо, чтобы дверь была связана с одной или двумя зонами доступа, для чего нужно сначала добавить соответствующие зоны доступа путем последовательного выбора требуемого плана зоны доступа и названия и индекса добавляемой зоны. При добавлении контролируемых дверей необходимо учитывать геометрическую привязку считывателя к двери для случаев использования Proximity карточки или ключа для открытия более одной двери. Чтобы привязать дверь к определенному считывателю, необходимо в режиме редактирования свойств двери указать в свойстве «Реле» реле прибора С2000-4, если добавляемое реле имеет номер 2, то необхо-

димо после сохранения информации о двери, привязать требуемую дверь к считывателю на странице «Структуры охранной системы» при условии, что у считывателя прибора С2000-4, реле которого указывается при геометрической привязке, свойство «Все двери» должно быть установлено как «Нет», после чего подтвердить произведенные действия для сохранения в базе данных.

При создании на плане объекта пожарных зон и размещения соответствующих извещателей следует использовать отдельный от охранных зон план помещения, т.е. при добавлении плана помещения его необходимо добавить 2 раза с разными названиями: первый — для пожарной подсистемы, второй — для охранной.

На четвертом этапе необходимо заполнить страницу структуры системы, предназначенную для отображения соответствия физической структуры охранной системы, определяемой на странице адресов приборов, и логической структуры системы, определяемой на странице планов охраняемых объектов.

На пятом этапе необходимо произвести ввод данных о персонале на странице ввода персонала, на которой кроме стандартных кнопок можно использовать кнопки, предназначенные для загрузки файла с фото сотрудника с диска компьютера или для непосредственного ввода фото сотрудника с теле или цифровой камеры, что возможно в том случае, если к компьютеру с системой подключены устройства оцифровки видеоизображения — видеоплаты или цифровые камеры. В результате в списке сотрудников будет изображение, которое можно будет видеть на странице управления персоналом, как показано на рис. 4.14.

На шестом этапе необходимо произвести Заполнение прав доступа сотрудника на странице определения прав доступа и паролей персонала. У каждого пользователя могут быть пароли для программного обеспечения, для клавиатуры С2000, для брелоков TouchMemory или Proximity карточек приборов С2000-4. Страница ввода паролей приведена на рис. 4.15.

The screenshot shows a web-based interface for managing employee data. On the left, there is a list of employees under the heading 'Сотрудники'. The employee 'Мельников А. М.' is selected. The main area contains a photo of the employee and a video placeholder. To the right, there are several input fields: 'Т. номер' (1), 'Фамилия' (Мельников), 'Имя' (Алексей), 'Отчество' (Михайлович), 'Статус' (Владелец), 'Раб. тел.' (33333), and 'Дом. тел.' (22222). Below these are dropdown menus for 'Компания' (Фирма), 'Подразделение' (Менеджеры), 'Должность' (Директор), and 'График работы' ([График работы подразделения]). There are also checkboxes for 'Свободный график' and 'Запрет перехода через сутки'. At the bottom, there is a field for 'Автомобиль' (Ока) and a row of buttons: 'Править', 'Добавить', 'Удалить', 'Печать', 'GSM', and 'Выход'.

Рис. 4.14. Ввод информации о сотруднике

The screenshot shows a web-based interface for configuring access rights for an employee. On the left, there is a list of employees under the heading 'Пароли сотрудников'. The employee 'Мельников А. М.' is selected. The main area contains a configuration panel for the selected employee. It includes a dropdown for 'Сотрудник' (Мельников А. М.), a dropdown for 'Тип кода' (Пароль для программ), and a text field for 'Код' (*). Below this, there is a section for 'Действителен' (Valid from) with a date range from 01.08.2001 to 31.07.2010. The 'Полномочия на запуск программ' (Program launch permissions) section includes several checked options: 'Мастер системы', 'Администратор базы данных', 'Доступ к картотеке', 'Доступ к охранно-пожарной системе', 'Оперативная задача', 'Управление отдельными зонами', 'Управление особо охраняемыми разделами', 'Изменение протокола событий', and 'Учет рабочего времени'. There is also a dropdown for 'Полномочия оператора' (Максимум). At the bottom, there is a row of buttons: 'Править', 'Добавить', 'Удалить', and 'Выход'.

Рис. 4.15. Страница ввода данных прав доступа сотрудников

Путем набора соответствующего пароля на клавиатуре С2000 сотрудник сможет брать или снимать с охраны соответствующие разделы. Пароли для Proximity карточек или брелоков TouchMemory являются соответствующими кодами карточек или брелоков. Когда истекают сроки действия введенных паролей, соответствующая запись окрашивается в красный цвет. То же самое касается и ввода биометрических данных с помощью биометрических считывателей.

На седьмом этапе определяются полномочий персонала по доступу на охраняемый объект и управлению разделами охраняемого объекта со следующими уровнями доступа: максимум (максимальный уровень доступа для сотрудника или группы сотрудников); запрет (данному сотруднику или группе сотрудников накладывается полный запрет на проход на обозначенную охраняемую территорию и на управление разделами охраняемой территории).

На данной странице с использованием соответствующих вкладок устанавливаются уровни доступа к точкам прохода, зонам доступа и управления соответствующими устройствами. Для точек доступа доступно свойство ANTIPASSBACK (запрета повторного прохода) выбором значения «Строгий», или «Временной» (если необходимо анализировать время последнего прохода человека через данную дверь), или «Мягкий» (если просто необходимо занести факт прохода в журнал событий). Для «Временного» задается интервал времени, после которого дверь будет разблокирована (время считается с факта последнего прохода человека через данную дверь). При задании полномочий сразу для нескольких точек доступа, объединенных зоной доступа в одну группу задействуется вкладка «Зоны доступа».

На восьмом этапе определяются сценарии управления, которые затем смогут запускаться с дерева управления в «Оперативной задаче» по заданному расписанию или по определенному событию в системе. Каждый сценарий управления состоит из определенных шагов, формируемыми «Шагом сценария».

Сценарии управления могут запускаться по возникновению определенных событий в системе, например, взятие, снятие раздела, тревожные события и пр.

Нельзя привязывать идентичный сценарий к идентичному событию, например, привязать сценарий взятия раздела № 1 к событию «Взятие раздела» того же первого раздела, что приведет к заикливанию программы. Рекомендуется добавить следующие 4 основных сценария: взятие раздела на охрану, снятие раздела с охраны, эвакуация, пожарная тревога, причем для каждого сценария должны быть определены соответствующие действия.

Сценарии управления могут запускаться как в ручном режиме, так и автоматически, через определенный интервал времени. Для задания времени запуска сценариев и служит страница формирования расписания запусков сценариев управления.

На девятом этапе определяются окна времени, в течение которых у сотрудника или группы сотрудников имеются права доступа на охраняемый объект или в зону доступа, как показано на рис. 4.16. Окна времени используются при задании уровней доступа сотрудников.

На десятом этапе необходимо сформировать дерево управления, с которого в Оперативной задаче можно будет в ручном режиме запускать сформированные сценарии управления. Далее задать расписание запусков сценариев управления, а также определить, необходимость запуска сценариев по определенным событиям системы, связав данные сценарии управления с событиями системы в Инспекторе.

На завершающем этапе работы с администратором баз данных осуществляется запись БД в пульт С2000, как показано на рис. 4.17, что необходимо для автономной работы системы без компьютера как в рабочем так и режиме настроек, а также необходимо обновить БД в «Оперативной Задаче» для работы в рабочем режиме на АРМе охранника.

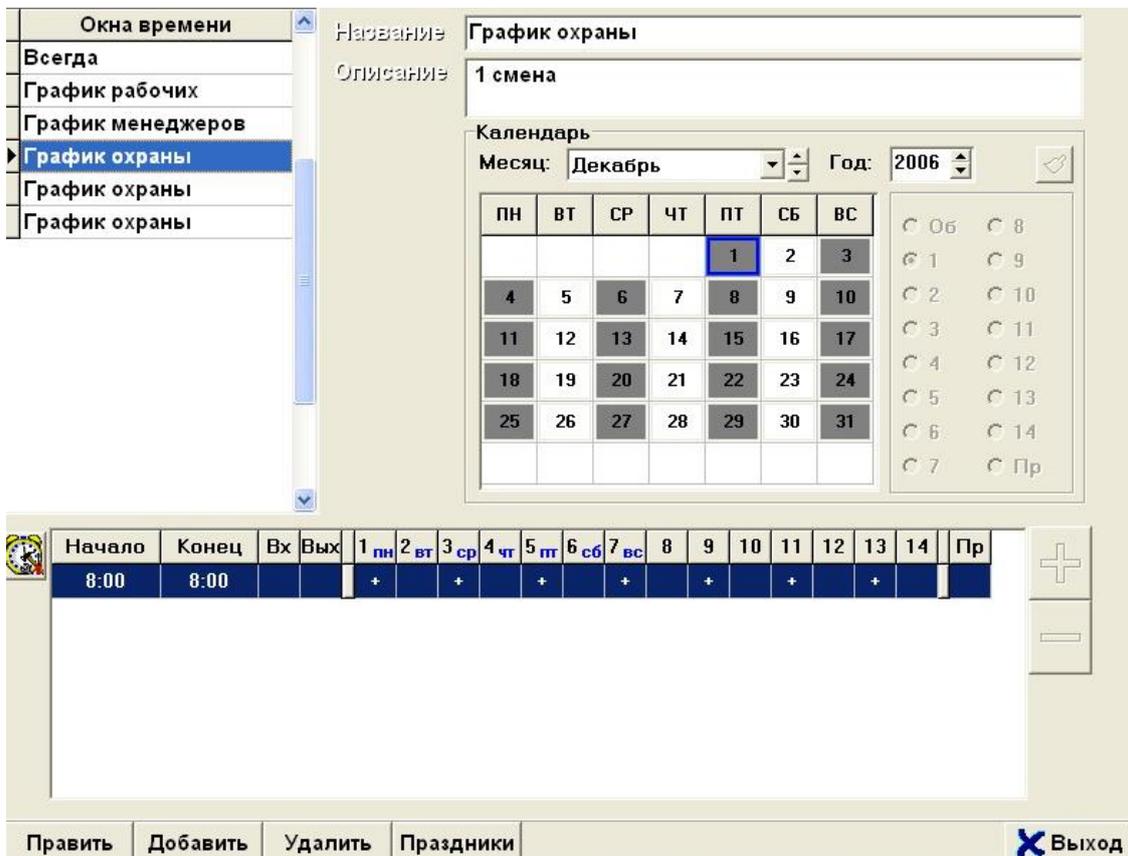


Рис. 4.16. Задание окон времени

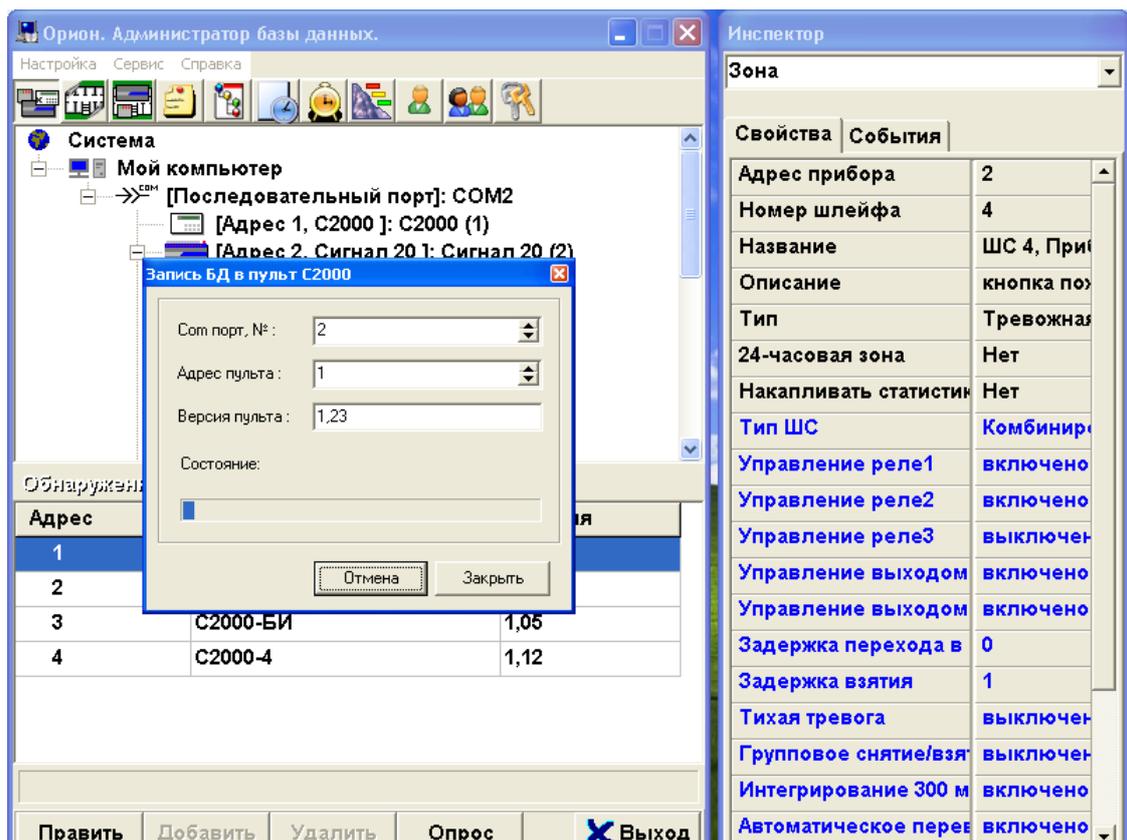


Рис. 4.17. Запись БД в пульт контроля и управления

Оперативная задача имеет основное свое предназначение для управления взятием на охрану и снятием с охраны объектов, и для удобства восприятия и работы с информацией данная программа имеет несколько страниц, каждой из которых соответствует кнопка-пиктограмма, расположенная на панели управления, как показано на рис. 4.18:

- страница графического отображения тревожного состояния;
- страница отображения Журнала Событий;
- страница управления взятием/снятием и опросом разделов.

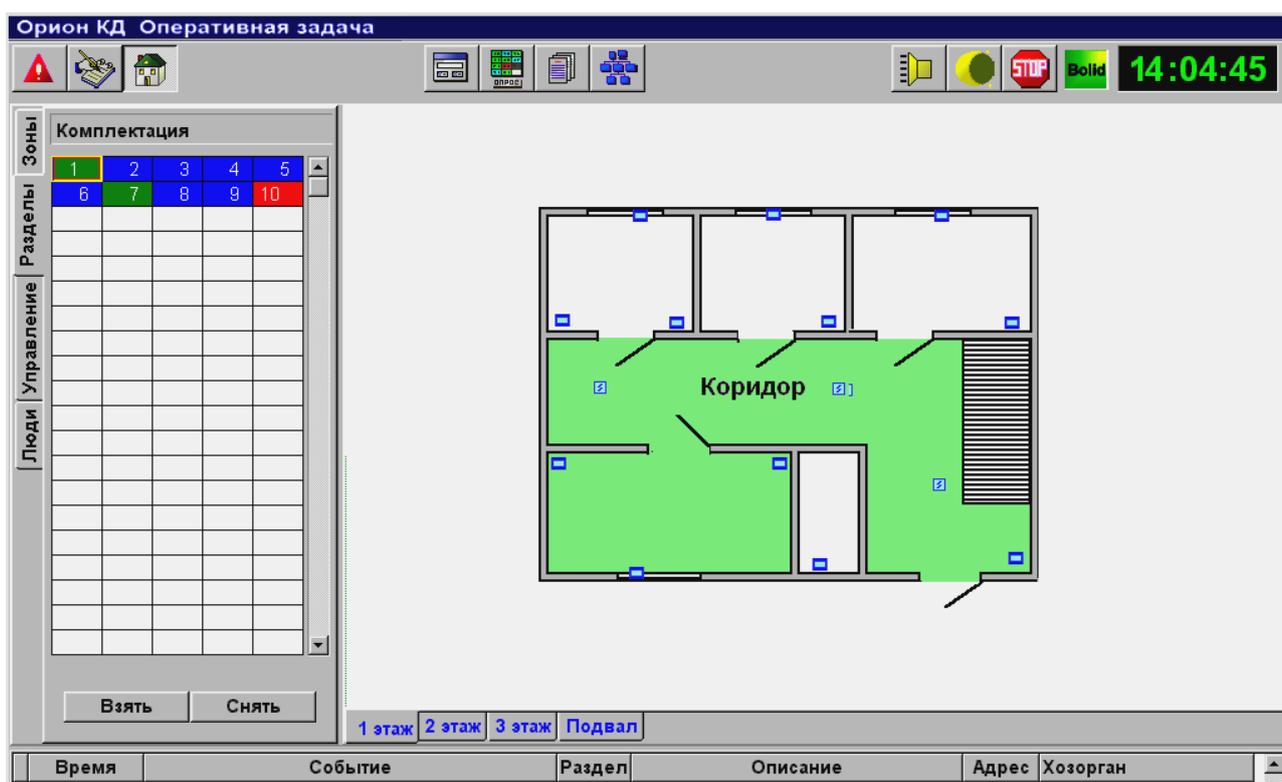


Рис. 4.18. Интерфейс оперативной задачи

Назначение кнопок на панели управления программы приведено в табл. 4.3. По щелчку клавиши мыши на области раздела, извещателе, элементе контроля доступа на планах помещений возникает локальное меню, выбирая пункты которого возможно управлять данным разделом, зоной, элементом или получить справку о данных объектах.

Страница тревожного состояния раздела может отображать такие группы тревог как текущие, обработанные, убранные в архив, переключение между вкладками которых позволяет отобразить соответствующие тревоги.

Таблица 4.3

Назначение кнопок панели управления Оперативной задачи

Вид кнопки	Функциональное назначение
	переключение на страницу графического отображения тревог
	переключение на страницу отображения «Журнала Событий»
	переключения на страницу опроса разделов
	запрос пароля оператора при смене дежурства
	опрос состояния разделов
	отображение списка подключенных приборов
	выключение сигнала тревоги
	включение хранителя экрана
	завершение работы и выход из программы
	оперативный отчет о дежурной смене

На странице для обработки тревог предусмотрены специальные кнопки, как показано в табл. 4.4.

Для обработки пришедшего тревожного события выполняются следующие действия:

- выбор тревоги из списка текущих тревог;
- нажатие кнопки «Снять с охраны»;
- направление группы задержания для нормализации тревожной ситуации;
- нажатие кнопки «Отметка высылки ГР» для пожарной тревоги, или «Отметка высылки ГЗ»;
- нажатие кнопки «Убрать в обработанные» при нормализации оперативной обстановки (данная тревога теперь будет отображаться на вкладке «Обработанные»).

Тревога с расставленными отметками будет иметь цвет, отличающийся от цвета только что пришедшей тревоги. Обработанные тревоги могут быть помещены в архив по аналогии с предыдущим перемещением.

Таблица 4.4

Кнопки обработки тревог

Название кнопки	Функциональное назначение
«Отметка вызова ГЗ»	отметка вызова группы задержания по текущей тревоге
«Отметка вызова НМ»	отметка вызова наряда милиции по текущей тревоге
«Отметка вызова ГР»	отметка вызова группы разведки по текущей пожарной тревоге
«Отметка вызова ПО»	отметка вызова пожарной охраны
«Снять с охраны»	снять с охраны раздел
«Перевзять»	перевзять раздел
«Сброс тревоги»	снятие тревожного состояния шлейфа
«Убрать в обработанные»	считать текущую тревогу обработанной
«Указать причину»	указать причину тревоги
«Убрать в архив»	убрать в архив обработанную тревогу

Взятие, снятие и опрос разделов производится на соответствующей странице при переключении на которую появляется окно с отображением разделов как в виде набора прямоугольников, так и в виде списка с соответствующими цветами состояния раздела. Для каждого состояния раздела определен свой цвет, как показано в табл. 4.5.

Таблица 4.5

Состояния раздела

Цвет	Состояние раздела
Зеленый	на охране
Синий	раздел снят с охраны
Коричневый	не взятие
Черный	нет связи
Красный	тревога

Для взятия раздела на охрану необходимо подвести курсор к прямоугольнику, номер которого соответствует номеру необходимого раздела и нажать левую кнопку мыши — данный прямоугольник будет обведен в рамку, после чего следует нажать на клавишу «Взять» — прямоугольник окрасится в цвет состояния на охране или, если команда не прошла, в одно из тревожных состояний. Для снятия раздела с охраны аналогично используется кнопка «Снять».

Контроль доступа и информация о сотрудниках осуществляется в окне оперативной задачи, как только определенный сотрудник или посетитель подносит карточку или ключ TouchMemory к считывателю, путем отображения фотографии данного сотрудника (текущая фотография выделяется рамкой, а предыдущая фотография без рамки и подсветки остается на экране некоторое время, пока не заместится следующей фотографией или, когда людской поток закончился, пока не истечет время показа фотографий, настраиваемое в «Администраторе БД») и срабатывания исполнительных устройств (турникета или замка) после проверки системой совпадения с занесенными в БД зна-

чениями кода ключа или карточки, временной зоны и таблицы праздников для данного сотрудника, а также привязки считывателя к конкретной двери.

Для получения более подробной информации о работе с системой необходимо ознакомиться с документацией ПО системы «ОРИОН» [15].

При проектировании систем безопасности немаловажную роль играет автоматизация данного процесса. Для данной цели служит программа NanoCAD «ОПС», которая автоматизирует проектирование подсистем, включая пожарную сигнализацию, охранную сигнализацию, оповещение, видеонаблюдение, а также СКУД для промышленных и гражданских объектов [20].

Ядро системы представляет платформа NanoCAD Plus — универсальная российская САПР, содержащая необходимые инструменты для базового проектирования и формирования чертежей, а также поддерживающая базы данных оборудования более 40 производителей охранно-пожарных систем, извещателей, систем оповещения и кабеленесущих систем и пр. [20], и в частности ИСБ «Орион». Все базы легко редактируются и пополняются с возможностью организации для группы пользователей общей сетевой библиотеки баз данных оборудования на сервере. При запуске программы локальные базы синхронизируются с сетевой базой, что позволяет работать даже без сетевого подключения.

Область применения программного комплекса NanoCAD ОПС — это проектирование «слаботочных» сетевых систем с учетом стандартов СП 5.13130.2009, СП 3.13130.2009, РД 25.953-90, РД 78.36.002-99, РМ 78.36.001-99, НПБ 160-97, ГОСТ Р 21.1101-2013 [20]. В NanoCAD «ОПС» осуществляется проектирование «с нуля» таких подсистем КСБ, как пожарной сигнализации, охранной сигнализации, контроля и управления доступом, видеонаблюдения, оповещения, кабельных каналов, порошкового и газового пожаротушения. NanoCAD ОПС не зависит от других графических систем и поддерживает формата DWG.

Основные функции NanoCAD «ОПС» следующие [20]:

- автоматическая расстановка на плане помещения пожарных, охранных извещателей, ПКП и оборудования СКУД;
- автоматическая расстановка на плане помещения видеокамер систем видеонаблюдения с выбором угла обзора;
- расчет токовой нагрузки;
- оценочный расчет кабеля для шлейфов сигнализации с осуществлением трассировки;
- расчет уровня звука речевых и звуковых оповещателей;
- формирование 3D-модели на основе расставленного оборудования и проложенных кабельных каналов;
- автоматическое формирование структурной схемы проекта с разбивкой по подсистемам;
- автоматическое формирование отчетных документов по отечественным стандартам для последующей выгрузки.

В рамках информационной модели NanoCAD «ОПС» позволяет автоматически расставлять пожарные извещатели по помещениям с учетом различных условий их установки и параметров согласно следующей нормативной документации:

- расстановка точечных пожарных извещателей согласно требованиям таблиц 13.3 и 13.5 раздела 13 СП 5.13130.2009;
- расстановка линейных дымовых пожарных извещателей согласно требованиям пп. 13.5.3 и 13.5.4 и таблицы 13.4 раздела 13 СП 5.13130.2009;
- расстановка точечных пожарных извещателей в пространствах фальшпола и подвесного потолка;
- расстановка точечных пожарных извещателей согласно требованиям п. 13.3.10 раздела 13 СП 5.13130.2009;
- учет условий расстановки точечных пожарных извещателей согласно требованию п. 13.3.3 раздела 13 СП 5.13130.2009;
- учет условий расстановки точечных пожарных извещателей согласно требованию п. 14.1 раздела 14 СП 5.13130.2009 (без учета примечания).

Система NanoCAD «ОПС» позволяет как автоматически, так и в ручном режиме расставить охранные извещатели и видеокамеры под заданными углами, а также оборудование СКУД, все контроллеры и ПКП определяя его состав и высоту установки для всего проекта с максимальной реалистичностью.

Расчет токовой нагрузки осуществляет оценку нагрузки на шлейфах, в РИП с требованиями к емкости аккумуляторных батарей, а также расчет падения напряжения в линии.

Расчет токовой нагрузки на РИП и емкости аккумуляторных батарей ведется от АКБ, добавленных к РИП с учетом типа подключения АКБ (параллельного или последовательного). Токовая нагрузка на шлейф и емкость АКБ РИП рассчитываются как в дежурном режиме работы системы, так и в режиме «Пожар», а токопотребление приборов и устройств — по максимальной и минимальной нагрузке.

Оценочный расчет кабеля позволяет подобрать параметры кабеля для шлейфов сигнализации при расставленном оборудовании и включении его в шлейфы с учетом переходов между этажами.

Функция создания шлейфов сигнализации трех типов: традиционный (неадресный), адресный и информационная линия, позволяет выполнить индивидуальные настройки с учетом подключенных адресных и неадресных извещателей в шлейфах, а в информационной линии — адресных и адресно-аналоговых извещателей и других адресных устройств. Кроме того, в программе осуществляется автоматическая трассировка кабеля по шлейфам сигнализации вдоль кабельных каналов с учетом порядка подключения извещателей в шлейф.

Система NanoCAD «ОПС» не только минимизирует ошибки при проектировании, но и автоматически формирует отчетные документы по отечественным стандартам для последующей выгрузки либо на поле чертежа, либо в Microsoft Office или OpenOffice следующих документов:

- рабочих чертежей поэтажных планов с автоматически промаркированным оборудованием и расставленными выносками, а также с возможностью добавления рамки по ГОСТ Р 21.1101-2013;
- спецификаций оборудования по ГОСТ 21.110-95;
- структурной схемы проекта с возможностью отображения по подсистемам;
- отчетных таблиц: таблица адресов, таблица шлейфов, таблица подключения распределительных коробок, таблица прокладки кабелей, таблица используемых УГО;
- отчетов по расчетам уровня звука оповещателей,
- расчетов углов и зон обзора видеокамер;
- расчетов емкости батарей РИП;
- кабельных журналов шлейфов сигнализации, линий электропитания, интерфейсных шлейфов;
- экспликаций помещений по ГОСТ 21.501-93.

Подготовка чертежей к печати осуществляется в Мастере печати nanoCAD, а для документов MS Excel и MS Word — соответственно в Диспетчерах печати MS Excel и MS Word.

Для детального изучения свойств системы необходимо формирование проектов подсистем, что является предметом отдельного рассмотрения, а для получения более подробной информации о работе с системой NanoCAD «ОПС» необходимо ознакомиться с документацией к ней [16].

4.3. Экспериментальное задание

1. Провести аппаратное конфигурирование системы Орион с использованием пульта контроля и управления.
2. Провести программное конфигурирование системы Орион с использованием мастера конфигурирования.
3. Создать план помещения объекта охраны.

4. Заполнить базу данных с использованием администратора баз данных системы Орион, руководствуясь основными этапами работы с администратором баз данных.

5. Ознакомиться с основными функциями оперативной задачи АРМ Орион.

4.4. Контрольные вопросы

1. Перечислить основные характеристики ИСО Орион.

2. Каков состав оборудования ИСО Орион в соответствии с основными группами устройств?

3. Каковы основные особенности подключения сетевых устройств ИСО Орион?

4. Как осуществляется аппаратное конфигурирование системы?

5. Перечислить состав программного обеспечения АРМ Орион.

6. Перечислить основной порядок действий при работе с АРМ Орион.

7. Как работает программный конфигуратор системы?

8. Что необходимо выполнить перед первым запуском администратора баз данных ИСО Орион?

9. Перечислить основные этапы работы с администратором баз данных АРМ Орион.

10. Где и как настраивается функция запрета повторного прохода в администраторе баз данных?

11. Пояснить работу со сценариями управления.

12. Пояснить основные особенности работы в оперативной задаче АРМ Орион.

13. Назвать известный инструмент автоматизированного проектирования ОПС и его основное назначение.

14. Перечислить основные функции NanoCAD «ОПС».

15. Какую токовую нагрузку позволяет оценить информационная модель системы NanoCAD «ОПС»?

16. Какие отчетные документы позволяет сформировать система NanoCAD «ОПС»?

ЛИТЕРАТУРА

1. *Магауенов, Р.Г.* Системы охранной сигнализации: основы теории и принципы построения. Учебное пособие для вузов. — М.: Горячая линия — Телеком, 2004.
2. *Шачнев, А.И.* Устройства и системы охранно-пожарной сигнализации. — Минск: УП Технопринт, 2001.
3. *Волхонский, В.В.* Проектирование систем охранной сигнализации. — СПб., 2017.
4. *Синилов, В.Г.* Системы охранной, пожарной и охранно-пожарной сигнализации. Учебное пособие. — М.: Академия, 2014.
5. *Кемпф, В.А.* Основы применения специальной техники в профессиональной деятельности сотрудника полиции: учебное пособие / В.А. Кемпф. — Барнаул: Барнаульский юридический институт МВД России, 2016.
6. Инструкция по монтажу системы контроля и управления доступом PERCo-SC-600.
7. Руководство пользователя ПО системы контроля и управления доступом PERCo-SC-600.
8. Руководство пользователя считывателем/контроллером BioTrax.
9. *Кухарев, Г.А.* Биометрические системы: Методы и средства идентификации личности человека. — СПб.: Политехника, 2001.
10. *Дамьяновски, Владо.* CCTV. Библия видеонаблюдения. Цифровые и сетевые технологии. — М.: ООО «Ай-Эс-Эс Пресс», 2006.
11. <http://cctvcad.com/rus/help>.
12. <http://cctvcad.com/Files/VideoCAD%20in%20CCTV%20focus%2028%20spread.pdf>.
13. http://www.cctvinfo.com/news_article.aspx?news_id=2532.
14. Инструкция для контрольной панели JA-82KRC.
15. Инструкция для беспроводного пульта управления JA-80F.
16. <https://bolid.ru/production/orion/>.

17. Руководство по эксплуатации прибора приемно-контрольного охранно-пожарного «Сигнал-20».
18. Руководство по эксплуатации блока приемно-контрольного охранно-пожарного «С2000-4».
19. Руководство по эксплуатации АРМ «Орион Про». ЗАО НВП «Болид», 2017.
20. <http://old.nanocad.ru/products/detail.php?ID=21468>.