ЛАБОРАТОРНЫЙ ПРАКТИКУМ

В.М.ЛОГИН
А.В.БУДНИК

ТЕХНИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ

Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Кафедра радиоэлектронных средств

В.М.Логин, А.В.Будник

ТЕХНИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ

ЛАБОРАТОРНЫЙ ПРАКТИКУМ
по курсу **Физические и аппаратные средства защиты информации и их проектирование**
для студентов специальности
I-38 02 03 «Техническое обеспечение безопасности»
всех форм обучения

Минск 2007

УДК 004.3(075.8)
ББК 32.885я73
Л 69

Р е ц е н з е н т :
зав. каф. МиС БГУИР,
канд. техн. наук, доцент В. А. Богуш

Логин, В. М.

Л 69 Технические системы безопасности : лаб. практикум по курсу «Физические и аппаратные средства защиты информации и их проектирование» для студ. спец. I-38 02 03 «Техническое обеспечение безопасности» всех форм обуч. / В. М. Логин, А. В. Будник. – Минск : БГУИР, 2007. – 64 с. : ил.

ISBN

Приводится описание четырёх лабораторных работ. Первая работа посвящена проектированию систем охранно-пожарной сигнализации, вторая – проектированию систем видеонаблюдения. В третьей лабораторной работе рассматриваются основные принципы проектирования систем контроля и управления доступом. В четвертой лабораторной работе изучаются методы проектирования биометрических систем безопасности.

УДК 004.3(075.8)
ББК 32.885я73

ISBN

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В последнее время технические системы безопасности все больше входят в нашу жизнь и постепенно становятся её неотъемлемой составляющей. Современные системы охранной и пожарной сигнализации, контроля доступа, мониторинга и диспетчеризации, а также биометрические системы безопасности достаточно сложны и в экстремальных ситуациях управляют всем инженерным оборудованием здания, обеспечивая сохранение жизни людей. Поддерживать их в постоянной готовности – чрезвычайно важная задача.

Данный курс лабораторных работ ставит своей целью помочь студентам развить практические навыки проектирования технических систем безопасности, необходимые для успешного усвоения курса «Физические и аппаратные средства защиты информации и их проектирование», а также для решения практических задач в ходе курсового и дипломного проектирования.

Курс лабораторных работ предполагается проводить с использованием программных пакетов «Юнитроник®» ЗАО «ЮНИТЕСТ», VideoCAD ООО «Орбита-Союз», StilPost™ компании StilSoft©и библиотек обработки речевого сигнала корпорации AudiTech.

Первая часть каждой лабораторной работы знакомит студентов с теоретическими принципами проектирования технических систем безопасности. Теоретический раздел дополняет материал соответствующего лекционного курса и является необходимым для выполнения цикла лабораторных работ. Во второй части даётся описание программных пакетов, соответствующих каждой из работ. Знакомство студентов с программными пакетами осуществляется в рамках вводного занятия к циклу лабораторных работ.

Предполагается, что студенты, приступающие к выполнению лабораторных работ, обладают навыками квалифицированных пользователей персональных компьютеров.

Суть каждой лабораторной работы сводится к созданию той или иной технической системы безопасности. Персонализация заданий к каждой лабораторной работе осуществляется по средствам выдачи преподавателем каждому студенту индивидуального задания – плана объекта.

Выполнение лабораторных работ предполагает домашнюю подготовку, включающую: изучение соответствующего теоретического материала курса, знакомство с программными пакетами, изучение методики проведения лабораторных работ, подготовку планов объектов.

Результаты выполнения и подготовленные отчеты по каждой лабораторной работе индивидуально предъявляются студентом преподавателю и защищаются с привлечением необходимого теоретического материала из данного лабораторного практикума и лекционного курса.

Лабораторный практикум составлен так, что совершенствование прикладных учебных программ не вызывает необходимости внесения изменений в его текст.

ЛАБОРАТОРНАЯ РАБОТА №1
ПРОЕКТИРОВАНИЕ СИСТЕМЫ ОХРАННО-ПОЖАРНОЙ СИГНАЛИЗАЦИИ

1.1. Цель работы

Изучить теоретические основы проектирования систем охранно-пожарной сигнализации и получить практические навыки проектирования данных систем с помощью адресно-аналоговой системы сигнализации «Юнитроник».

1.2. Теоретические сведения

Современные системы охранно-пожарной сигнализации (ОПС) выполняют функции сбора и обработки информации, управления системами автоматического тушения пожара и инженерными системами здания. Одним из важнейших элементов систем сигнализации, которая определяет уровень развития этой техники, являются пожарные извещатели. Извещатели измеряют величину контролируемого фактора пожара и передают информацию на приемно-контрольный прибор (ПКП).

С появлением и развитием микроконтроллеров стало возможным создавать в извещателях эффективную систему самотестирования на основе контроля аналогового (непрерывно изменяющегося) значения фактора опасности. Система самотестирования извещателя должна контролировать не только отказы детектора извещателя, но и блока логической обработки сигнала, электрических цепей формирования выходных сигналов, цепей встроенного и выносного индикаторов. При этом сигнал подтверждения исправности должен прекращаться при частичном или полном отказе извещателя. Полный отказ обычно связан с отказом микроконтроллера или блока питания извещателя.

В настоящее время на потребительском рынке предлагается оборудование ОПС, использующее в своей работе технологии быстрого восстановления неисправностей. В основе этих технологий лежит разработанная на фирме новая концепция надежности аппаратуры, ориентированная на потребности эксплуатации оборудования и позволяющая обеспечивать надежность работы, близкую к идеальным требованиям. Данная концепция базируется на двух условиях, выполнение которых позволяет создавать системы сигнализации быстрого восстановления:

1. Извещатели и другие устройства в системе должны быть снабжены системой самодиагностики.

2. Извещатели и другие устройства должны передавать сигнал, подтверждающий их исправность, на пульт дежурного оператора.

В настоящее время разработаны извещатели с подтверждением исправности, предназначенные для работы в адресно-аналоговой системе сигнализации ЮНИТРОНИК®.

Данные извещатели являются аналоговыми извещателями с внешней адре-

сацией: адрес извещателя определяется шлейфом сигнализации (ШС), в котором он установлен. Это извещатели с упрощенной инсталляцией – они не требуют настройки и программирования параметров. Извещатели просты в эксплуатации, выдают извещения на ПКП о своей неисправности, о необходимости очистки от пыли и компенсируют влияние пыли на точность измерения. Извещатель при неисправности выдает сообщение на ПКП понятным для него языком: размыкает ШС, в результате ПКП выдает извещение «Неисправность» или «Обрыв шлейфа». Такое простое решение позволяет извещателю полноценно работать с любыми лучевыми ПКП – отечественными и импортными и при этом допускает установку одного извещателя в помещении вместо двух обычных.

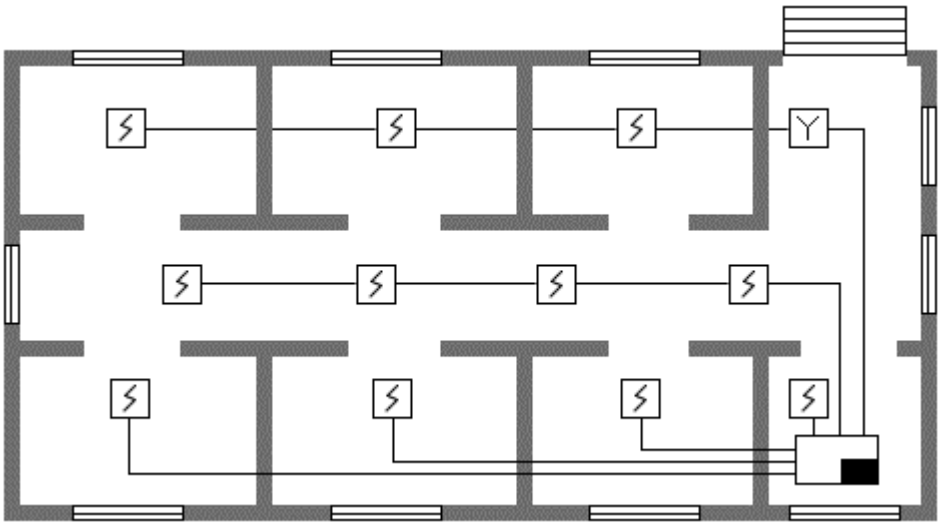

Рис. 1.1. Варианты установки извещателя.

На рис. 1.1 показаны два варианта установки одного извещателя в помещении. В первом случае в ШС устанавливается только один извещатель, при этом адрес извещателя соответствует адресу шлейфа. В тот же ШС допускается включать и другие извещатели, например, ручной. Во втором случае в ШС устанавливается несколько извещателей, причем каждый из них – один в помещении. Идентификация неисправного извещателя осуществляется по его оптическому индикатору или по подключенному к нему выносному устройству оптической индикации.

Приборы со знакопеременными ШС предоставляют лучшие возможности для работы извещателя: в случае неисправности одного извещателя в ШС остальные сохраняют свою работоспособность, а ПКП «Юнитроник 496» даже выдает специальный сигнал о неисправности извещателя, отличный от других сигналов («Обслуживание»).

1.3. Техническое описание ППКОПУ «Юнитроник 496»

1.3.1. Назначение и возможности

Прибор приемно-контрольный охранно-пожарный и управления ППКОПУ «Юнитроник 496» (далее АПКП) в составе адресно-аналоговой системы сигнализации «Юнитроник» предназначен для централизованной и автономной охраны зданий и сооружений – офисов, магазинов, банков, складских помещений, жилых домов, учреждений, предприятий от несанкционированных проникновений и пожаров.

АПКП предназначен:

- Для сбора и обработки информации о проникновении, пожаре или неисправностях от пожарных и охранных извещателей (ПИ и ОИ), извещателей состояния (ИС), а также о неисправностях шлейфов сигнализации и других устройств, входящих в состав системы сигнализации;
- Для оповещения дежурного персонала о возникших событиях путем выдачи текстовых, световых и звуковых сообщений на встроенный и дополнительно подключаемый малогабаритный дисплей, а также на выносные устройства оповещения, русифицированный принтер и компьютер с сохранением сообщений в энергонезависимой памяти АПКП;
- Для управления устройствами пожаротушения (УП) и дымоудаления.

АПКП может работать как автономно, так и в составе сети, объединяющей несколько приборов в единую охранно-пожарную систему, с выводом информации на компьютер.

Доступ к управлению системой обеспечивается персонифицированными электронными ключами (Touch Memory или карты Proximity). Общее количество ключей доступа не должно превышать 384 на один прибор.

Журнал событий АПКП обеспечивает хранение не менее 1790 последних событий с указанием вида происшествия, времени и даты, а также типа извещателя, назначения ключей доступа и имени их владельцев. Информация в памяти сохраняется при отключении основного и резервного питания в течении не менее 10 лет.

В приборе имеется возможность устанавливать текущее время и дату, просматривать журнал событий, подключать новые и удалять ненужные ключи доступа, извещатели и модули адресации, управлять текущим состоянием прибора.

Обслуживание компонентов системы производится по требованию самой системы и только указанных ею извещателей, модулей и участков шлейфа.

Система проста в эксплуатации, содержит минимальное число клавиш управления. Построение меню и система подсказок сводят управление к последовательности простых, интуитивно понятных действий, не требующих специального обучения персонала.

Органы управления и индикации АПКП показаны на рис. 1.2.

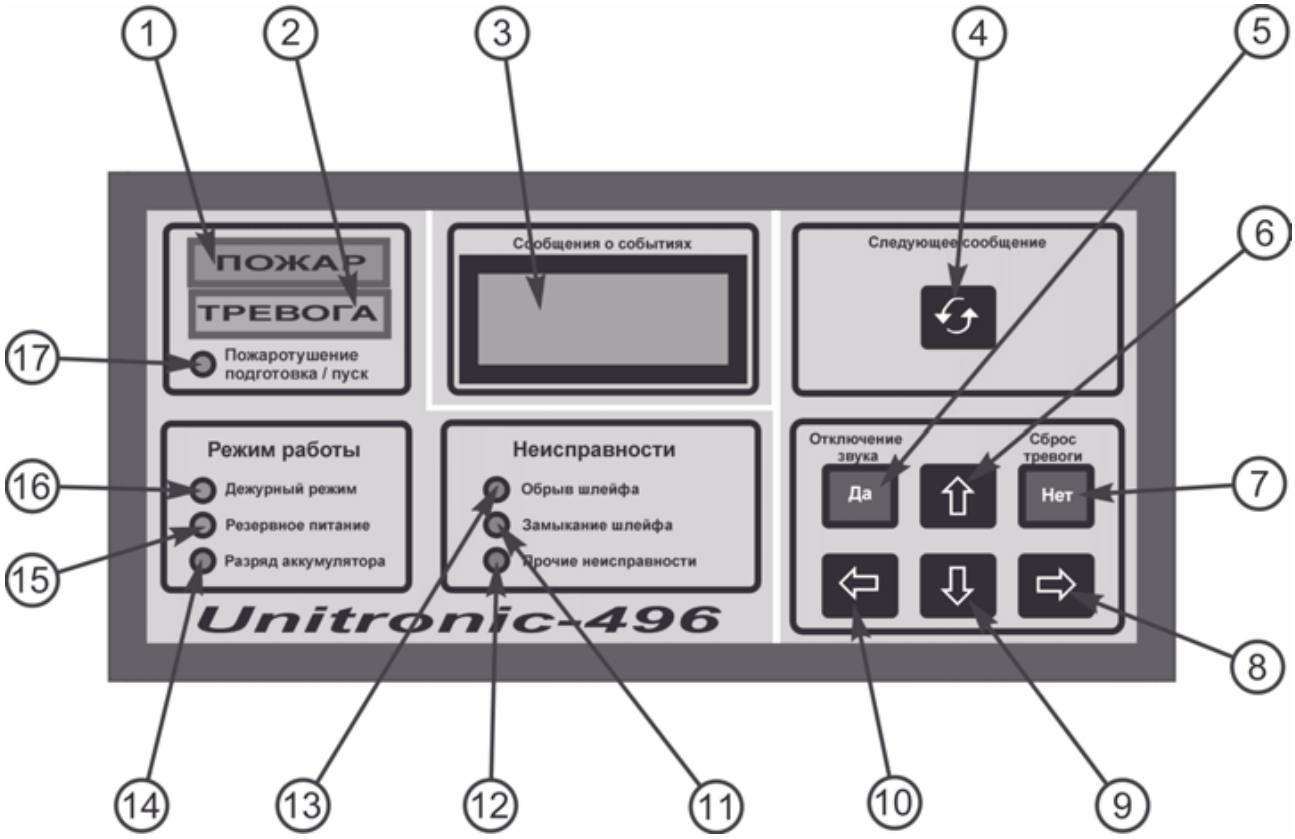

Рис. 1.2. Органы управления и индикации АПКП:

1 – индикатор красного цвета «ПОЖАР»; 2 – индикатор желтого цвета «ТРЕВОГА»; 3 – ЖК дисплей; 4 – кнопка просмотра буфера событий с индикатором наличия информации в буфере; 5 – кнопка «Отключение звука» («Да»); 6, 8 ... 10 – кнопки выбора направлений; 7 – кнопка «Сброс тревоги» («Нет»); 11 ... 13 – индикаторы неисправностей: замыкание шлейфа, прочие неисправности, обрыв; 14 ... 16 – индикаторы режима работы АПКП: разряд аккумулятора, режим резервного питания, дежурный режим; 17 – индикатор состояния УП: подготовка / пуск

1.3.2. Состав АСПС «Юнитроник»

На базе АПКП возможно сформировать адресную систему пожарно-охранной сигнализации (АСПС). Для этого к информационным линиям АПКП в произвольном порядке и в удобном месте подключаются адресные устройства, тип и назначение которых представлены в табл. 1.1.

Таблица 1.1

Список устройств, подключаемых к АПКП

№ пп	Наименование, тип устройства	Назначение
1	Извещатель пожарный дымовой адресно-аналоговый ИП 212-49А.	1. Измерение уровня дыма в точке установки. 2. Самодиагностика, контроль дымового канала. 3. Контроль и компенсация запыленности.
2	Модуль управляющий МА-У.	Управление устройствами охранной и пожарной автоматики: 1. Выход реле (переключающие контакты 5А, 220В); 2. Контроль цепи управления и питания одного устройства; 3. ШС для контроля состояния исполнительного устройства.
3	Модуль управляющий МА-У4.	Управление устройствами охранной и пожарной автоматики: 1. 4 выхода реле (переключающие контакты 5А, 220В); 2. Контроль цепей управления и питания устройств; 3. Последовательное срабатывание реле с интервалом 0 ... 90 сек.
4	Адресная метка управления оповещением, пожаротушением МА-УОП.	Управление устройствами охранной и пожарной автоматики: 1. Выход реле (переключающие контакты 3А, 24В); 2. Контроль шлейфа управления несколькими устройствами.
5	Адресная метка охранно-пожарная и контрольная МА-7ТК.	1. Контроль шлейфа сигнализации с пожарными, охранными или извещателями состояния с НЗ-контактным выходом. 2. Различает одно и два срабатывания в шлейфе. Максимальное количество охранных извещателей – 8 шт., пожарных – 20 шт.
6	Адресная метка пожарная: МА-7ТС, дополнительное питание 24В; МА-7ТС.12, питание 12В; МА-7ТСН, питание 24В.	1. Контроль шлейфа сигнализации с пожарными извещателями с токовым выходом, контроль изъятия извещателей. 2. Различает одно и два срабатывания в шлейфе.

Окончание табл. 1.1

		3. Обеспечивает сброс тревоги дымовых извещателей путем кратковременного отключения их питания. Ток потребления извещателей в дежурном режиме – до 1 мА (для МА-7ТСН – от 1 до 2 мА).
7	Адресная метка пожарная: МА-7ТСУ, питание 24В; МА-7ТСУ.12, питание 12В.	То же, что МА-7ТС, имеет дополнительный выход управления сиреной (открытый коллектор 200 мА) при срабатывании извещателей в своем ШС.
8	Модуль адресации охранно-пожарный МА-РК, питание 24В (12В).	1. Контроль считывателя Touch Memory (Proximity) для постановки/снятия объекта с охраны или включения автоматики пожаротушения. 2. Контроль шлейфа сигнализации с пожарными, охранными или извещателями состояния с контактным выходом. Максимальное количество охранных извещателей – 8 шт., пожарных – 20 шт.
9	Размыкатель линии РЛ-1.	1. Изолятор короткозамкнутого участка информационной линии. 2. Ответвитель линии.

1.3.3. Рекомендации по проектированию АСПС «Юнитроник»

1.3.3.1. Определение основных параметров системы. АСПС «Юнитроник» является системой с распределенной логикой, что обеспечивает гибкость её архитектуры и возможность создавать структуру управления, сбора и обработки информации, максимально приспособленную к архитектуре объекта.

Каждое сигнальное адресное устройство (АУ) контролирует только один шлейф сигнализации, который программно устанавливается в охранный, пожарный или контрольный режим работы. Управляющие АУ имеют также выходы для управления внешними устройствами с контролем цепей управления и программируются на срабатывание по различным событиям в системе.

В системе заложены типовые шаблоны поведения и приемы инсталляции, облегчающие её проектирование и последующее программирование.

Рекомендуется определить основные параметры системы в следующей последовательности:

1. Руководствуясь типовыми правилами технического содержания установок пожарной автоматики и строительными нормами и правилами, в соответствии с техническим заданием и Руководством по проектированию АСПС «Юни-

троник», разместить на плане здания необходимое количество пожарных и охранных извещателей.

2. Определить тип и необходимое число АУ для обеспечения требуемой информативности, не превышая допустимое количество извещателей на один шлейф сигнализации (см. табл. 1.1). Рекомендуется использовать не менее одного АУ на помещение и при возможности применять адресно-аналоговые пожарные извещатели (АПИ), обеспечивающие более высокую надежность работы системы сигнализации.

3. Определить требуемое количество сигналов управления устройствами пожарной автоматики (УПА). Исходя из этого выбрать тип и количество управляющих АУ, а также количество датчиков контроля состояния устройств (открыто / закрыто, включено / выключено и т.п.).

Датчики состояния могут быть подключены к любому АУ в контрольном режиме работы, однако для контроля состояния управляемых устройств удобно использовать дополнительный вход для подключения шлейфа сигнализации, которым снабжены управляющие АУ.

4. Для дистанционного управления включением / выключением пожарной автоматики на объекте, снятия / постановки объекта на охрану необходимо предусмотреть вблизи помещения считыватели Touch Memory или Proximity, а также контроллеры считывателей МА-РК.

5. Объединить АУ в группы («объекты») для группового снятия / постановки на охрану, управления пожарной автоматикой. Каждое АУ в системе обязательно должно быть программно размещено в одном из «объектов», который, как правило, соответствует помещению, пожарной или охранной зоне. В последующем информация о событиях в системе будет привязана к именам этих объектов.

Возможна программная установка одного сигнального АУ одновременно в нескольких объектах. Срабатывание извещателей в шлейфе сигнализации такого АУ приводит к возникновению события во всех указанных объектах. Необходимо иметь в виду, что свободное адресное пространство в АПКП при этом сокращается на число использованных адресов.

Установка одного управляющего АУ в нескольких объектах запрещается.

6. Для построения системы противопожарной автоматики в АПКП предусмотрены три уровня управления:

· по событию в данном объекте;

· по событию в любом из объектов в выделенной группе объектов («группе УПА»);

· по событию в любом из объектов АПКП.

Группы УПА формируются исходя из потребности управления устройствами, общими для нескольких объектов (лифтами, вентиляторами, заслонками системы дымоудаления и т.д.).

Для управления устройствами, общими для всех объектов АПКП, в приборе предусмотрены 4 реле с переключающими контактами и выход «ОК».

7. Срабатывание реле или открытого коллектора управляющих АУ может

быть программно задано по возникновению следующих событий в объекте:

– срабатывание охранного извещателя («Проникновение»);

– постановка на охрану;

– срабатывание автоматического пожарного извещателя («Пожар-1»);

– срабатывание ручного либо двух автоматических пожарных извещателей («Пожар-2»);

– окончание отсчета времени после события «Пожар-2» («Пожар-2 с задержкой»);

– окончание отсчета времени в любом из объектов заданной группы УПА («Пуск УПА»);

– при включении автоматического режима работы пожарной автоматики (для включения таблички «Автоматика включена»).

Шлейф сигнализации, который подключен к управляющему АУ, всегда относится к объекту, в котором это АУ установлено, в то время как управляющий выход АУ может быть запрограммирован как на срабатывание по событию в своем объекте («Проникновение», «Пожар-1», «Пожар-2», «Пожар-2 с задержкой», «Автоматика включена»), так и по событию в любом объекте группы УПА («Пуск УПА»).

Для соблюдения правильной последовательности отработки устройств пожарной автоматики необходимо учитывать, что сначала происходит срабатывание управляющих АУ, запрограммированных на событие в своем объекте («Пожар-2 с задержкой»), а затем – на событие в группе УПА («Пуск УПА»).

8. Срабатывание реле или открытого коллектора АПКП может быть программно задано по возникновению перечисленных в п. 7 событий в АПКП, а также по событиям «Пожар / Тревога» – для управления сиреной или событию «Неисправность».

9. Определить требуемое число АПКП исходя из условий:

– число АУ в одной информационной линии не должно превышать 86 (с учетом резерва адресов в каждой линии не менее 10% для последующего наращивания системы);

– число объектов не должно превышать 128 на один АПКП;

– количество групп УПА не должно превышать 8 на один АПКП.

10. Определить наиболее подходящее место расположения АПКП так, чтобы максимальное удаление адресных устройств от любой из клемм АПКП по длине информационной линии не превышало 1000 м (см. подпункт 1.3.2.4).

11. Выбрать схемы включения информационных линий: «луч», «кольцо» или «кольцо с ответвлениями». При этом следует иметь в виду, что кольцевая схема обеспечивает более высокую надежность работы системы за счет сохранения связи с устройствами при одиночном обрыве информационной линии. Структура линии «кольцо с ответвлениями» обладает наиболее высокой защищенностью, т.к. позволяет сохранять связь с устройствами при множественных обрывах в ответвлениях. При этом кольцевая часть линии должна быть проложена в защищенных местах с ограниченным доступом.

1.3.3.2. Управление пожаротушением. В АПКП предусмотрены шаблоны поведения для формирования управления работой установок газового, аэрозольного, порошкового пожаротушения.

Для реализации этих алгоритмов помимо пожарных извещателей и устройств пуска и контроля состояния технологических установок необходимо предусмотреть на объекте световую индикацию (таблички «Газ уходи», «Газ не входи», «Порошок уходи», «Порошок не входи», «Автоматика включена»), считыватель Touch Memory или Proximity для дистанционного включения / выключения автоматического режима работы установки, датчик открытия двери для выключения автоматического режима, кнопку дистанционного пуска.

Для контроля шлейфов пожарной сигнализации, контроля кнопки дистанционного пуска, датчика открытия двери, технологических датчиков (давления, веса и т.д.) необходимо использовать необходимое число сигнальных АУ.

Для каждой цепи пуска и таблички системы пожаротушения необходимо предусмотреть управляющее АУ. Для контроля считывателя Touch Memory (Proximity) следует установить модуль адресации МА-РК.

Для подключения шлейфов пожарной сигнализации, технологических датчиков, датчика двери можно использовать незадействованные контрольные входы управляющих АУ и модуля МА-РК. При этом необходимо учитывать, что управляющие АУ не обеспечивают контроль шлейфа на обрыв и короткое замыкание.

1.4. Конфигурирование системы с использованием компьютера

Подключить прибор к свободному COM порту компьютера, используя стандартный 0-модемный кабель. Инсталлировать в компьютер и запустить программу «Конфигуратор» в соответствии с её описанием.

Если прибор был уже частично конфигурирован, например, в автономном режиме, то рекомендуется получить базу данных из прибора и сохранить её на жестком диске.

Используя средства интерфейса компьютера и описание программы «Конфигуратор», отредактировать имеющуюся или создать новую конфигурацию пожарно-охранной системы и сохранить её на жестком диске.

Загрузить полученный файл конфигурации в прибор. Проверить работу прибора в автономном режиме.

1.4.1. Программа «Конфигуратор»

Программирование прибора можно осуществлять с приборной панели, но наиболее удобным является программирование с помощью программы «Конфигуратор», окно которой представлено на рис. 1.3.

Программа предназначена для:

– чтения конфигурации из памяти прибора и записи в прибор;

– создания и корректировки баз данных «Объекты», «Адресные устройства», «Ключи доступа»;

– синхронизации часов и календаря с ПЭВМ;

– контроля ошибок инсталляции;

– чтения журнала событий и их сортировки;

– вывода на печать журнала событий;

– вывода на печать конфигурации объекта;

– обновления версии программного обеспечения прибора.

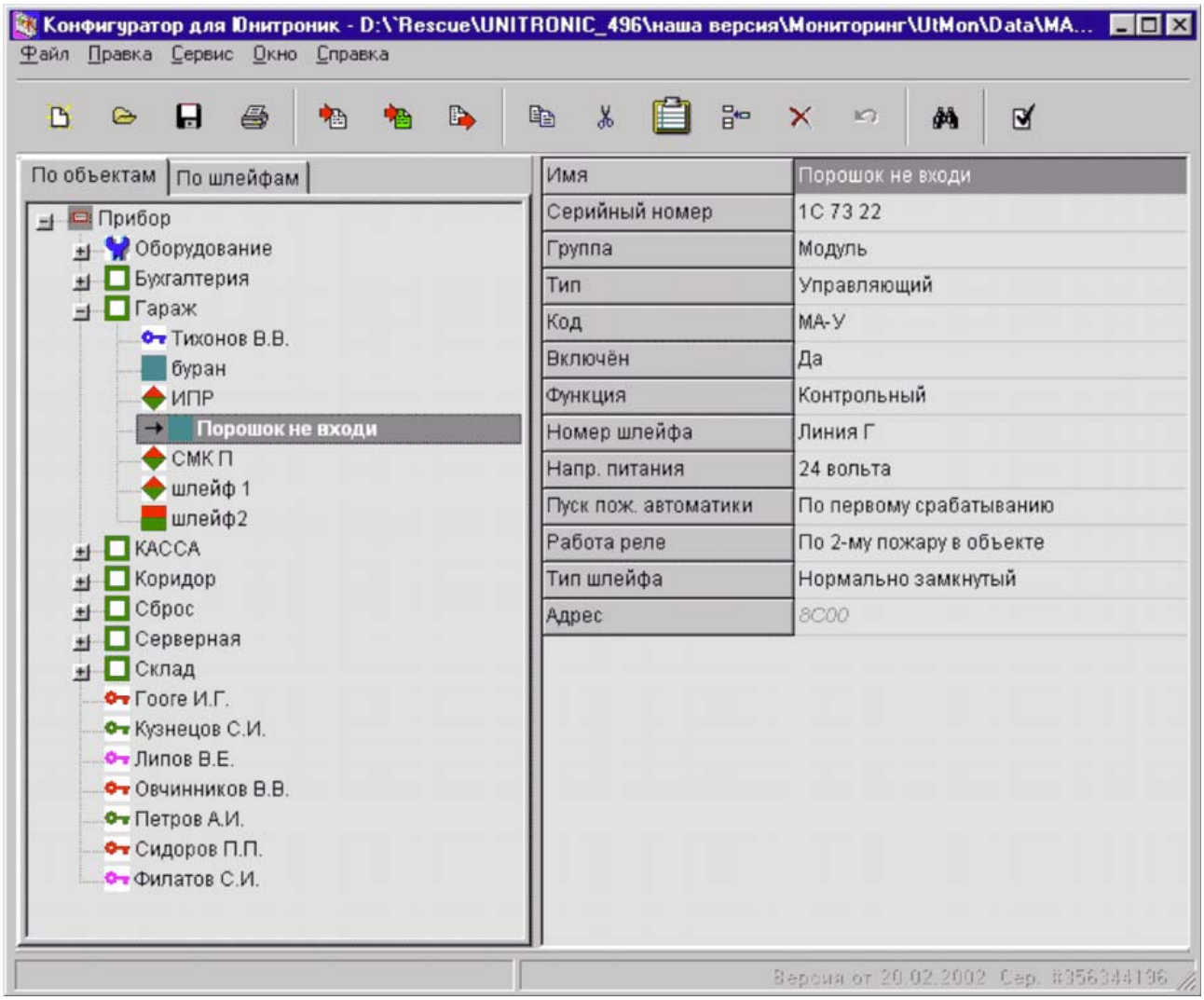

Рис. 1.3. Окно программы конфигуратора.

1.4.2. Программа «Мониторинг»

Программа «Мониторинг», окно которой представлено на рис. 1.4, предназначена для:

– объединения нескольких приборов с целью создания единого рабочего места дежурного;

– визуализации поэтажных планов;

– сбора информации о произошедших тревогах, неисправностях и других событиях;

– выдачи инструкций дежурному при тревоге и других событиях;

– постановки и снятия помещений с охраны;

– управления пожарной автоматикой;

– связи с другими ПЭВМ с использованием локальных сетей.

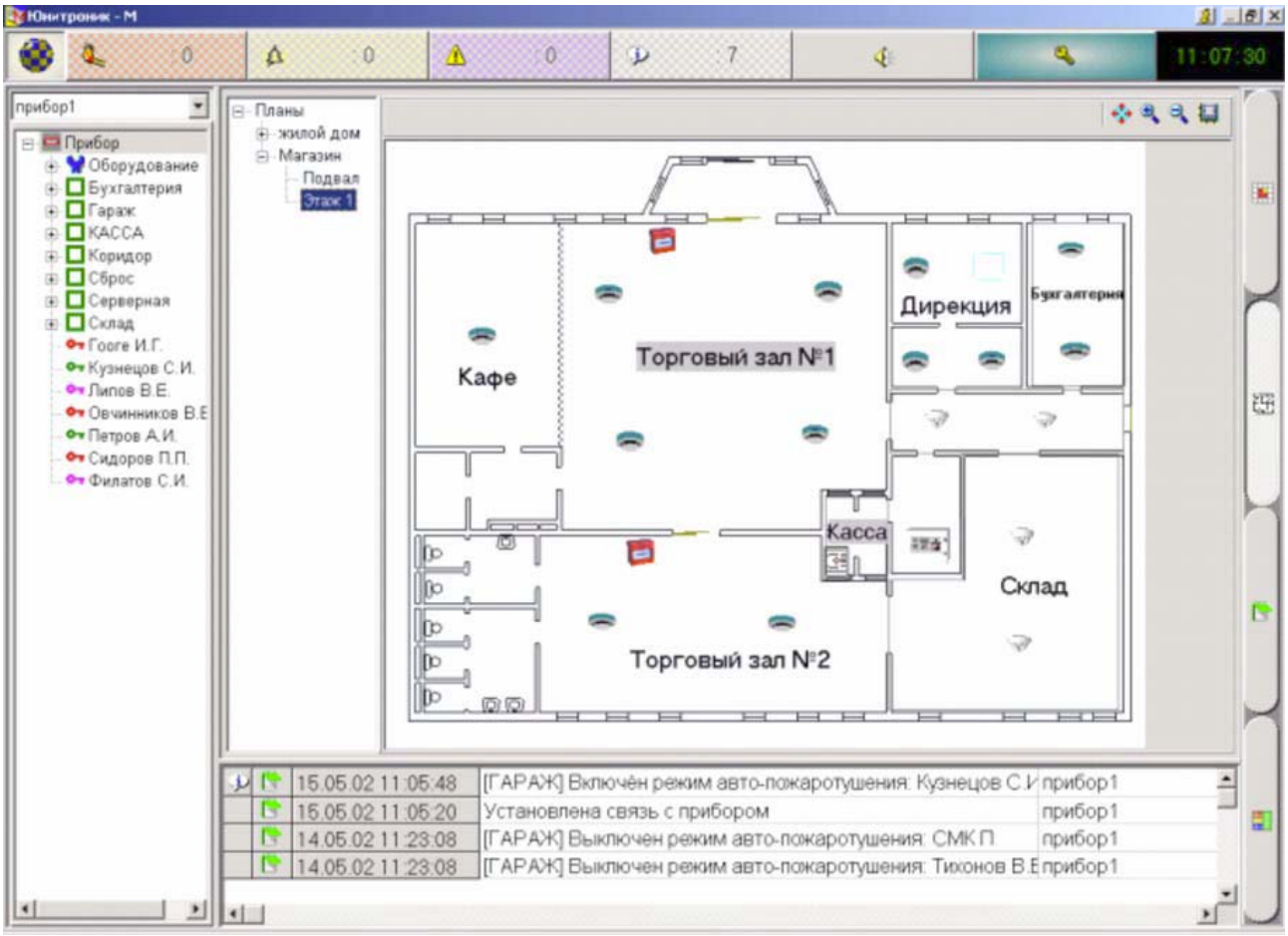

Рис. 1.4. Окно программы мониторинга.

1.5. Контрольные вопросы

1. Какие функции выполняют современные системы ОПС?

2. Для чего служат пожарные извещатели?

3. Что должна контролировать система самотестирования пожарного извещателя?

4. Что лежит в основе технологии быстрого восстановления, разработанной российской фирмой ЗАО «ЮНИТЕСТ»?

5. Какие аналоговые извещатели являются извещателями с внешней адресацией и в чём их достоинство?

6. Какие варианты установки одного аналогового извещателя с внешней адресацией в помещении вам известны?

7. Для чего предназначен АПКП «Юнитроник 496»?

8. Какие адресные устройства могут быть подключены к информационным линиям АПКП для формирования АСПС?

9. Какие основные параметры АСПС «Юнитроник» необходимо определить, для того чтобы спроектировать АСПС на выбранном объекте?

10. Что необходимо предусмотреть на объекте установки АСПС для реализации шаблонов поведения формирования управления работой установок газового, аэрозольного, порошкового пожаротушения?

11. Каким образом осуществляется конфигурирование АСПС «Юнитроник» с использованием компьютера?

12. Для чего предназначена программа «Конфигуратор»?

13. Для чего предназначена программа «Мониторинг»?

1.6. Задание

1. Изучить техническое описание ППКОПУ «Юнитроник 496», а также справку для конфигуратора и мониторинга ЮНИТРОНИК.

2. Получить у преподавателя план объекта.

3. С помощью программы «Конфигуратор для ЮНИТРОНИК» создать новую конфигурацию системы ОПС для полученного плана объекта согласно рекомендациям по проектированию АСПС «Юнитроник», приведённых в пункте 1.3.3. Сохранить файл с базой на жестком диске.

4. Загрузить полученный файл конфигурации в программу «Мониторинг для ЮНИТРОНИК». Проверить работу системы в автономном режиме.

5. Показать выполнение лабораторной работы преподавателю.

1.7. Содержание отчета

1. Цель работы.

2. Распечатка созданной конфигурации базы прибора из программы «Конфигуратор для ЮНИТРОНИК».

3. Схема размещения оборудования разработанной системы ОПС. Пример оформления схемы размещения представлен в приложении А на рис. А.1, а графические представления условных обозначений приборов в табл. А.1.

4. Конкретные предложения по снижению затрат на проектирование и монтаж удобной архитектуры системы ОПС в соответствии с планом выбранного объекта.

5. Выводы по работе.

ЛАБОРАТОРНАЯ РАБОТА №2
ПРОЕКТИРОВАНИЕ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

2.1. Цель работы

Изучить теоретические основы проектирования систем видеонаблюдения и получить практические навыки проектирования данных систем с использованием программы проектирования телевизионных систем VideoCAD.

2.2. Теоретические сведения

2.2.1. Возможности, преимущества и область применения систем видеонаблюдения

Благодаря постоянно растущим потребностям в большей безопасности и рационализации сегодня не существует области повседневной жизни, в которой не применяются видеосистемы. При этом видеотехника используется самостоятельно или в сочетании с другой техникой.

В простейшем случае можно установить телевизионную систему наблюдения из одной или нескольких камер, которые предают изображения на один или несколько мониторов. Однако сегодняшняя тенденция ведет все больше и больше к установкам, выполненных в виде комплекта системной техники, при использовании которого благодаря участию интеллектуального центрального блока возможна связь с внешними системами. Это может быть система охраны здания, система для сигнализации об опасности, открытая охранная система или система контроля доступа, представленные на рис. 2.1.

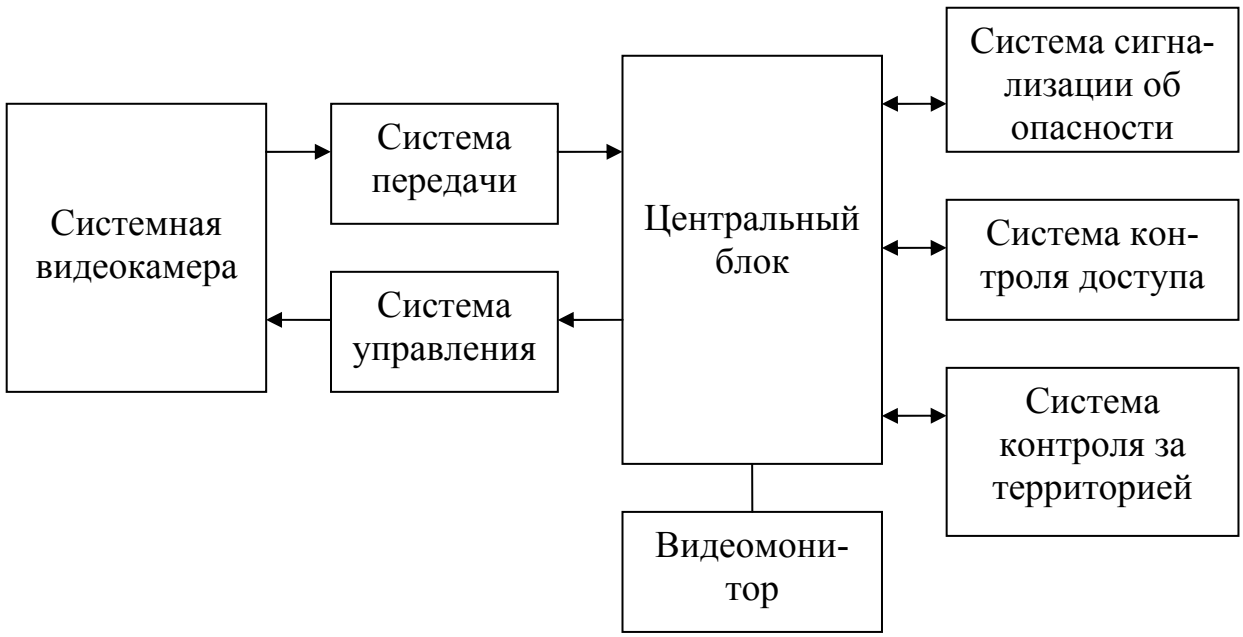

Рис. 2.1. Структурная схема системной видеотехники.

Самостоятельно или в сочетании с другой техникой видеосистемы наблюдения предоставляют следующие возможности и преимущества:

– распознавание и локализация опасности;

– проведение мероприятий по управлению и регулированию;

– предотвращение ущерба;

– документирование и анализ нарушений.

На практике имеет значение следующее:

– сокращение опасностей для персон и ценностей;

– быстрое реагирование при опасностях, угрозах или нарушениях;

– распознавание ложных тревог без дополнительных персональных затрат;

– экономия затрат.

Для обеспечения безопасности видеосистемы применяются в следующих случаях:

– наблюдение за воротами, контроль входа;

– контроль за территорией и объектами (склады, охранные зоны и т.д.);

– безопасность экспонатов в музеях, картинных галереях и на выставках;

– контроль документов на неохраняемом входе;

– дистанционное наблюдение в финансовых учреждениях и магазинах;

– контроль за служебными помещениями с целью предотвращения хищений;

– применение в охране окружающей среды (надзор за отработавшими газами и сточными водами);

– применение на автобусах и больших транспортных средствах (контроль за дверьми, наблюдение позади транспортного средства);

– наблюдение за гаражами (открытыми автостоянками);

– наблюдение за шлюзами в судоходстве;

– наблюдение за аэропортами и рулежными дорожками;

– наружные и внутренние устройства пожарной сигнализации;

– скрытое наблюдение при невидимом инфракрасном освещении.

Рационализация применения видеосистем заключается в следующем:

– целенаправленное персональное применение при наблюдении за служебными помещениями и ремонтными предприятиями;

– управление транспортными потоками в уличном движении, на перекрестках, в туннелях и т.д.;

– передача документов, изображений, фотографий, чеков и т.д.;

– применение в машинах, таких как, например, перемещение электрода в сварочных аппаратах, подача ленты на барабан на прокатном стане, наблюдение за ленточным транспортером, контроль за уровнем наполнения силосной башни и т.д.;

– передача показаний приборов с автоматической метеостанции;

– автоматический контроль за выходом продукции, например, за процессами разлива и наклейки этикетки;

– применение в химической атмосфере, контроль за этапами разливки, контроль за этапами производства, использующими взрывчатые вещества, передача изображений с очистных сооружений и т.д.;

– замедленный просмотр быстро протекающих процессов в полиграфической и текстильной промышленности;

– визуальная помощь при монтаже маленьких деталей.

Видеосистемы применяются и в измерительной технике:

– бесконтактное измерение длин и площадей;

– сравнение цвета и помутнения при заданных значениях;

– телевизионная микроскопия;

– телевизионная эндоскопия;

– телевизионная осциллография;

– передача измеренных данных;

– цифровая вставка измеряемых значений в телевизионное изображение (например, время, частота вращения, масса, давление и т.п.);

– аналоговая вставка измеряемых значений в телевизионное изображение;

– вставка измерительной метки, например, при наличии контакта или достижении упора при управлении слябингом на прокатном стане.

Возможно использование видеосистем в науке и медицине:

– телевизионные приемы в ускоренной и замедленной съемке,

– телевизионная микроскопия и эндоскопия;

– глазные исследования (флуоресцентная ангиография);

– усиление и передача рентгеновских изображений;

– дистанционная передача анализов;

– изучение поведения в психиатрии;

– исследования потоков и турбулентностей;

– демонстрация и регистрация слабо светящихся явлений в физике;

– наблюдение за пациентами в больницах.

2.2.2. Проектирование видеосистемы

Важнейшим шагом в разработке концепции видеосистемы является по возможности строгий анализ потребности заинтересованной стороны, будущей работы установки и особенностей, специфических для проекта. При этом надо определиться по виду проверочного списка, пример которого представлен в табл. 2.1.

Подобный банк данных, дополненный при необходимости эскизами, должен быть составлен во время первой консультации и обсуждения информации с заинтересованной стороной, именно в присутствии её представителей. Чаще всего уже на этом этапе появляется возможность, которую обязательно следует использовать, установления корреляции между истинной потребностью, возможно уже имеющимися готовыми концептуальными представлениями и ра-

циональной реализуемостью. При этом в большинстве случаев одновременно возникает еще и хорошая возможность для консультации и приобретения нужной базовой информации. Оказывается исключительно полезным, когда в этом обсуждении принимают участие сотрудники заинтересованной стороны, которые позже должны работать с установкой или отвечать за её применение.

При этом могут быть ликвидированы предубеждения и обсуждены субъективные аспекты использования.

Таблица 2.1

Необходимая информация, указания и данные
для разработки концепции видеосистемы

Что нужно прояснить?	Возможные результирующие решения / заданные величины.
О каком типе объекта идет речь?	Применение стандартного видео / средняя опасность / высшая ступень защиты.
Сколько камер нужно в общей сложности и на каждый отдельный участок?	Число необходимых камер определяется из индивидуального анализа слабости положения охраняемого объекта.
Сколько наружных / внутренних камер нужно установить?	Зависит от соответствующей необходимой комплектации.
Сколько камер нужно с постоянной, жесткой установкой?	Постоянное расположение необходимого горизонтального угла обзора для оптимального охвата объекта и возможность распознавания.
Сколько камер нужно использовать на дистанционно управляемых головках с изменяемой пространственной ориентацией? Позиционирование: да / нет.	Выбор подходящих дистанционно управляемых систем и минимального / максимального угла обзора трансфокатора.
Как велико расстояние передачи в центр для каждой отдельной камеры? Сколько мест наблюдения / обслуживания необходимо? В каком месте нужно использовать центральный блок? Необходимо ли объединение систем сигнализации и систем контроля входа?	Выбор подходящей системы передачи и необходимых устройств. Основные критерии для выбора соответствующих центральных блоков.
Являются установленные специальные приборы целесообразными или обязательными?	Видеосенсоры, цифровая видеопамять, квадратор, мультиплексор, видеопринтер, видеомагнитофон с длительным временем записи.

Вскоре после этого обсуждения консультант должен будет в своем бюро проанализировать полученные данные, чтобы определить точный объем системы, оптимально соответствующий потребностям.

Важным в этой связи является соответствующая классификация типов установок, представленных на рис. 2.2, чтобы можно было сделать правильный выбор оборудования специфического использования.

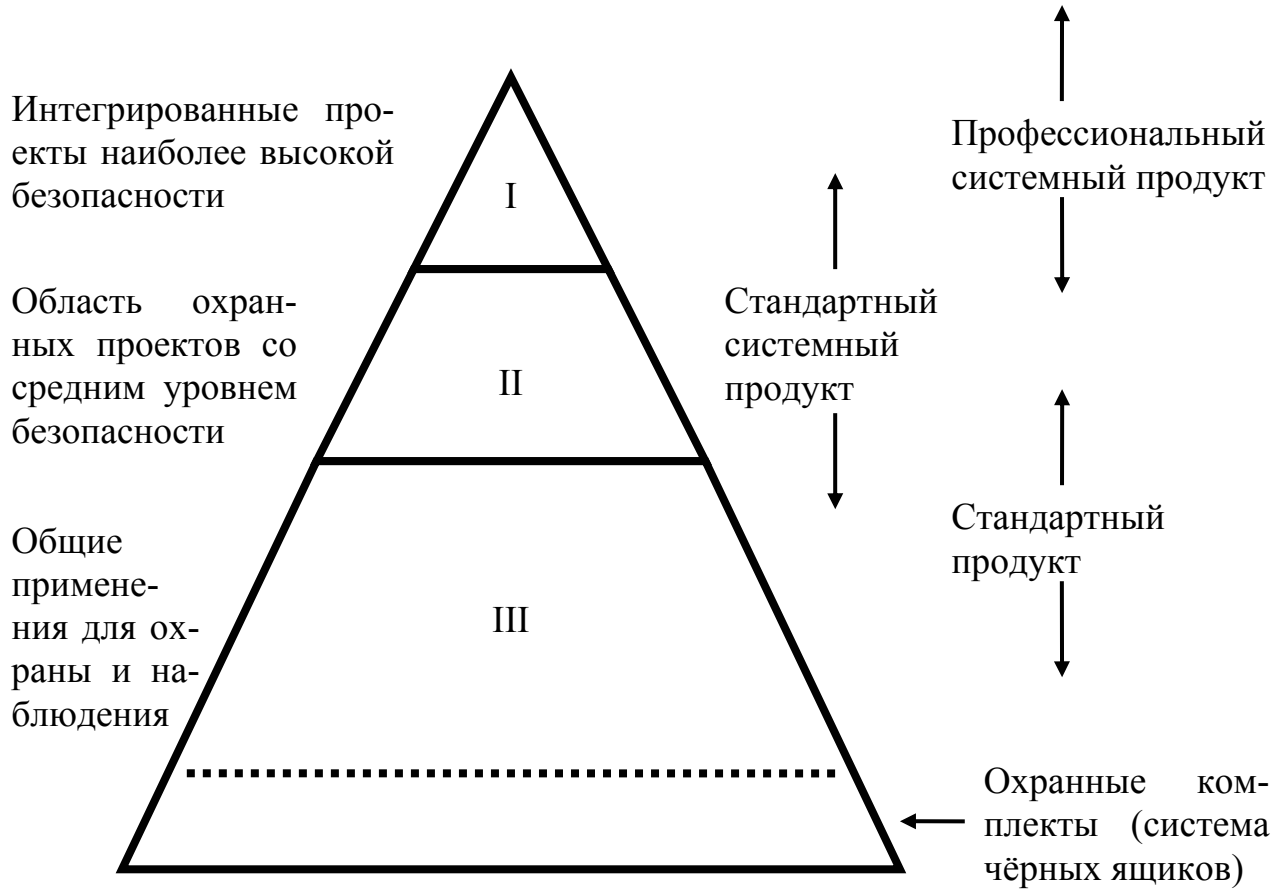

Рис 2.2. Типы видеоустановок и представление их продукции.

Сама схема видеоустановки в системе (см. рис. 2.1) показывает, что при проектировании установки такого рода функционально установленные решения должны все время попадать в цель или приниматься во внимание установленные критерии выбора.

В качестве преобладающих аспектов для установки должны быть приняты во внимание специальные аспекты из области безопасности.

2.2.2.1. Проектирование практической схемы. Каждое проектирование видеоустановки предполагает с одной стороны по возможности строгий анализ потребностей в безопасности при будущем использовании, с другой стороны требует обширных базовых технических, физических знаний проектировщика.

Только при этих условиях возможна выработка индивидуальных, связанных с потребителем, системных предложений, в случае необходимости с аль-

тернативными вариантами, которые в дальнейшем оптимально выполняют все установленные требования на практике.

После представления всех фактов, имеющих значение для потребностей в безопасности, нужно провести все необходимые шаги проектирования в соответствии со схемой, составленной компанией Philips CSS. Схема, представленная на рис. 2.3, показывает различные фрагменты видеоустановки, выполненные на базе распределенной системной техники. Одновременно разъясняется, как неизбежны многие уникальные решения при проектировании установок такого рода.

Указания по применению универсальной схемы проектирования видеоустановок:

Продвигайтесь, как указано, соблюдая последовательность шагов по следующей схеме проектирования.

При наличии системы с большим числом камер часто приходится многократно повторять определенные шаги проектирования, так как они в сфере безопасности являются обычно общими, например, относительно различных мест монтажа камеры, угла обзора камеры, передающей техники.

При последовательном систематическом прохождении схемы вы ничего не пропустите и при помощи данных о системе и отдельных блоках всегда сможете принять правильное решение.

Если в проекте определенные группы блоков или критериев выпадают или не нужны, пропустите их и следуйте далее по указанным шагам проектирования.

2.2.2.2. Шаги проектирования видеосистемы. Шаги проектирования видеосистемы в деталях заключаются в следующем:

- Сначала выберите (1) соответствующий для каждого предусмотренного места монтажа тип камеры, который в каждом случае оптимально подходит для конкретной постановки задачи.
- Заданные величины (2), идет ли речь о A. – внутренней ориентации или B. – наружной ориентации, определены при выборе необходимой комплектации камер. Этот пункт должен быть рассмотрен также индивидуально для каждой камеры, т.к. во многих вариантах конфигурации оборудования, как для внутренних, так и для наружных камер он существует. Ниже на соответствующих шагах, в частности в 2A или 2B, вы найдете указания к принятой в расчет комплектации.
- Следующее решение A. – жесткий монтаж или B. – монтаж на головке с изменяемой пространственной ориентацией служит критерием для (3) применяемых монтажных приспособлений, (4) типа применяемого объектива и (5) при известных условиях дополнительно необходимых монтажных приспособлений.

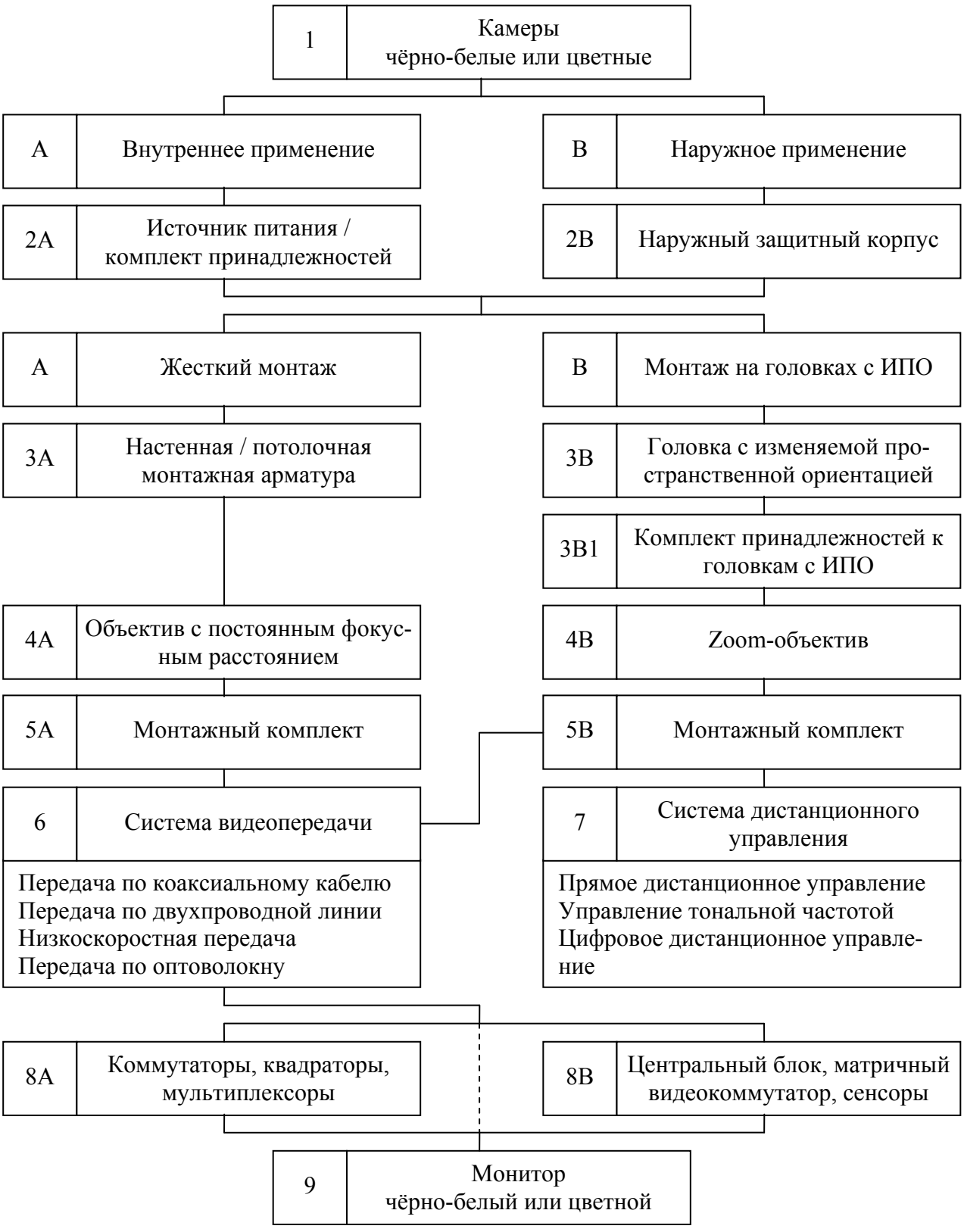

Рис. 2.3. Схема проектирования видеоустановки.

• Вне зависимости, имеется ли наружная или внутренняя ориентация, жесткий монтаж или монтаж на головке с изменяемой пространственной ориентацией, (6) нужно выбрать подходящую систему передачи видео.

• Для камер, которые должны работать на головках с изменяемой пространственной ориентацией (ИПО), (7) нужно выбрать оптимально подходящую систему дистанционного управления. Уже со сложившимся представлением о выборе коммутационного оборудования и центрального блока следует приступить к поиску интегральных системных решений. Если для решения предлагаются, например, системный видеокоммутатор, маленький матричный коммутатор видеосистемы или комплексный матричный коммутатор для видеомодулей, то при соответствующем предложении профессиональной системной видеотехники вы сможете найти подходящее комплексное решение.

• Далее осуществляется выбор таких (8) устройств, как квадраторы, мультиплексоры, сенсоры и т.д.

• На заключительном этапе необходимо правильно выбрать (9) видеомонитор, а также место для его установки или расположения.

2.2.3. Выбор места монтажа камеры

Во многих случаях в первую очередь рекомендуется выполнить рисунок с расположением камер, по которому можно определить горизонтальный угол обзора камеры и из него фокусное расстояние объектива.

2.2.3.1. Примеры внутреннего монтажа камер. В принципе для всех внутренних применений камер справедлив подход, суть которого заключается в том, что место монтажа камер нужно выбирать так, чтобы в поле зрения камер не попадали окна и по возможности лампы. Это совершенно необходимо, т.к. регулировка диафрагмы объектива автоматически устанавливается на самую большую освещенность в кадре, и все остальные детали изображения будут воспроизводиться темными.

Выбор места монтажа камер для наблюдения за входом в помещение и за охраняемым объектом представлен на рис. 2.4.

На этом примере указано, как в помещении с охраняемым объектом нужно выбирать расположение камер для четкого наблюдения за входом и объектом. Угол обзора камеры, направленной на дверь, при известных условиях должен быть выбран немного больше, так чтобы входящие в помещение люди немного дольше находились в зоне видимости камеры. Однако угол обзора не должен быть существенно увеличен, т.к. для надежной идентификации желательно по возможности более крупноформатное изображение.

Выбор места монтажа камер для наблюдения в супермаркете представлен на рис. 2.5.

На данном рисунке показан типичный средней величины супермаркет со своими критическими зонами. Прежде всего, это зона касс, зона расположения наиболее дорогих товаров, таких как склад и зона приема товара. Дополнительно наблюдение ведется также за зоной, прилегающей к кассам со стороны выхода.

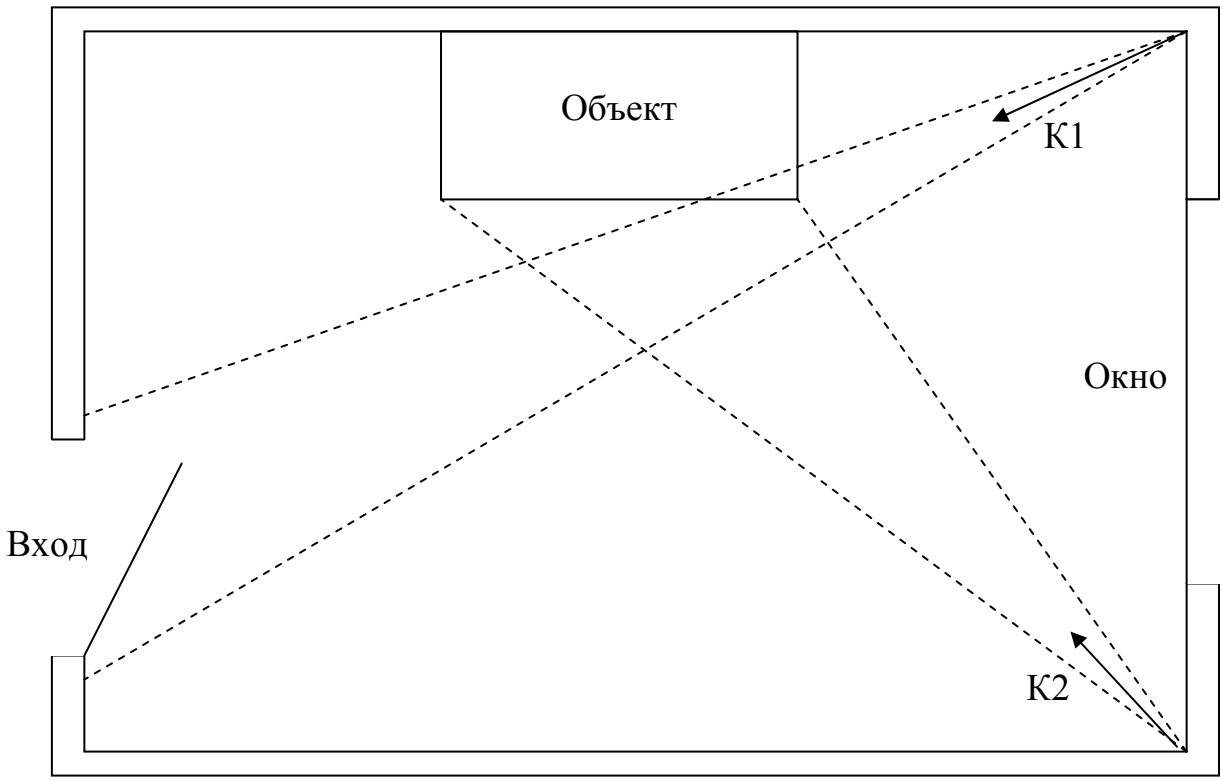

Рис. 2.4. Наблюдение за входом в помещение.

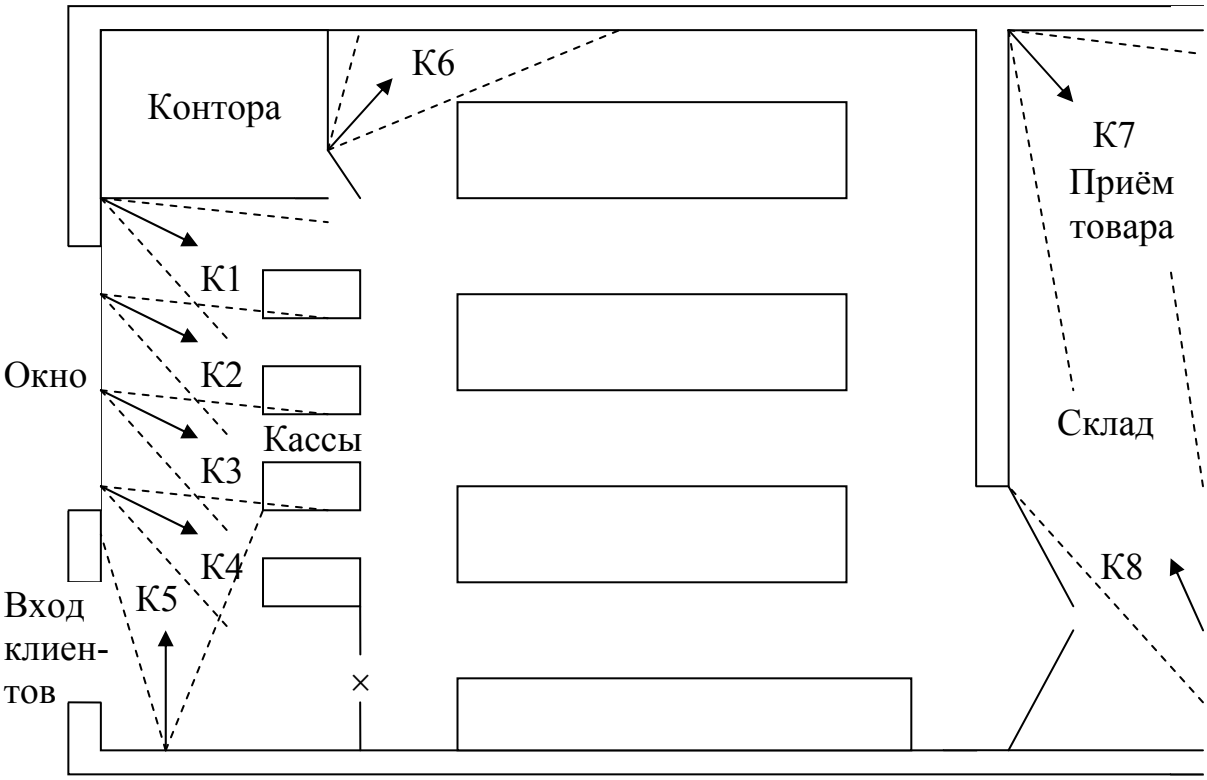

Рис. 2.5. Наблюдение в супермаркете.

Также здесь становится ясным, как с помощью правильного выбора мест монтажа размер и одного угла обзора может быть достигнут обзор всех опасных зон практически без пробелов.

Дополнительные замечания: в этом случае видеозапись с помощью 8-кратного мультиплексора была бы, несомненно, рациональным дополнением для реконструкции и анализа нарушений.

2.2.3.2. Примеры наружного монтажа камер. Выбор места монтажа камер для наблюдения за въездом во двор и автостоянкой для посетителей представлен на рис. 2.6.

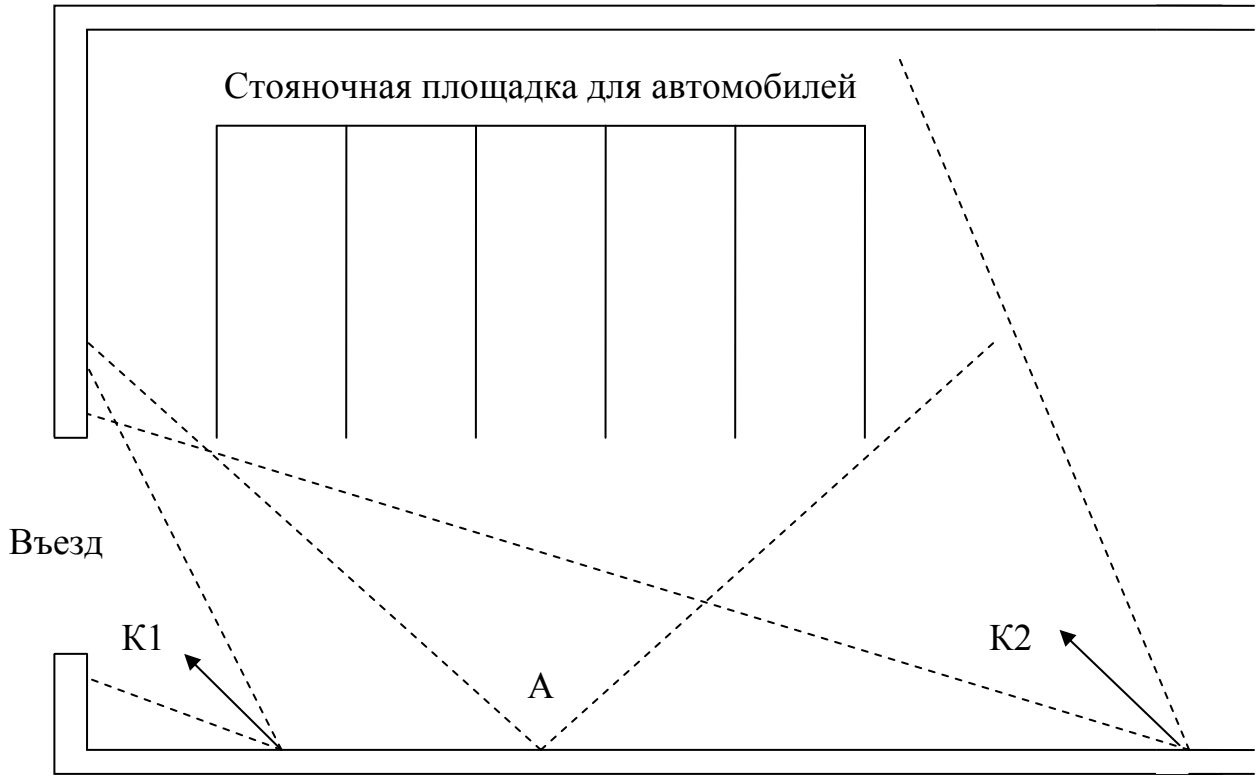

Рис. 2.6. Наблюдение за въездом во двор или автостоянкой для посетителей.

Камера К1 охватывает здесь въезд, в то время как камера К2 направлена на места стоянки легковых автомашин.

В условиях ограниченного размера объекта возможен другой выбор мест монтажа: например, К1 в точке А при соответствующем угле обзора другого объектива. К2 в точке А было бы более худшим вариантом, т.к. в этом случае пришлось бы использовать экстремально широкоугольный объектив. Результатом этого были бы геометрические искажения (эффект рыбьего глаза) и очень маленькое изображение всех автомобилей.

Выбор места монтажа камер для наблюдения за входом и подъездами к земельному участку представлен на рис. 2.7.

С обозначенной позиции камеры охватываются одновременно и вход и въезд. Если нужно только наблюдать за движением человека то место монтажа

А остается неизменным, необходимо лишь изменить основное направление камеры и выбрать объектив с соответствующим малым углом обзора.

При этом гарантируется достоверная идентификация человека.

Для отчетливого наблюдения за входом возможно также расположение места монтажа камеры в точке В.

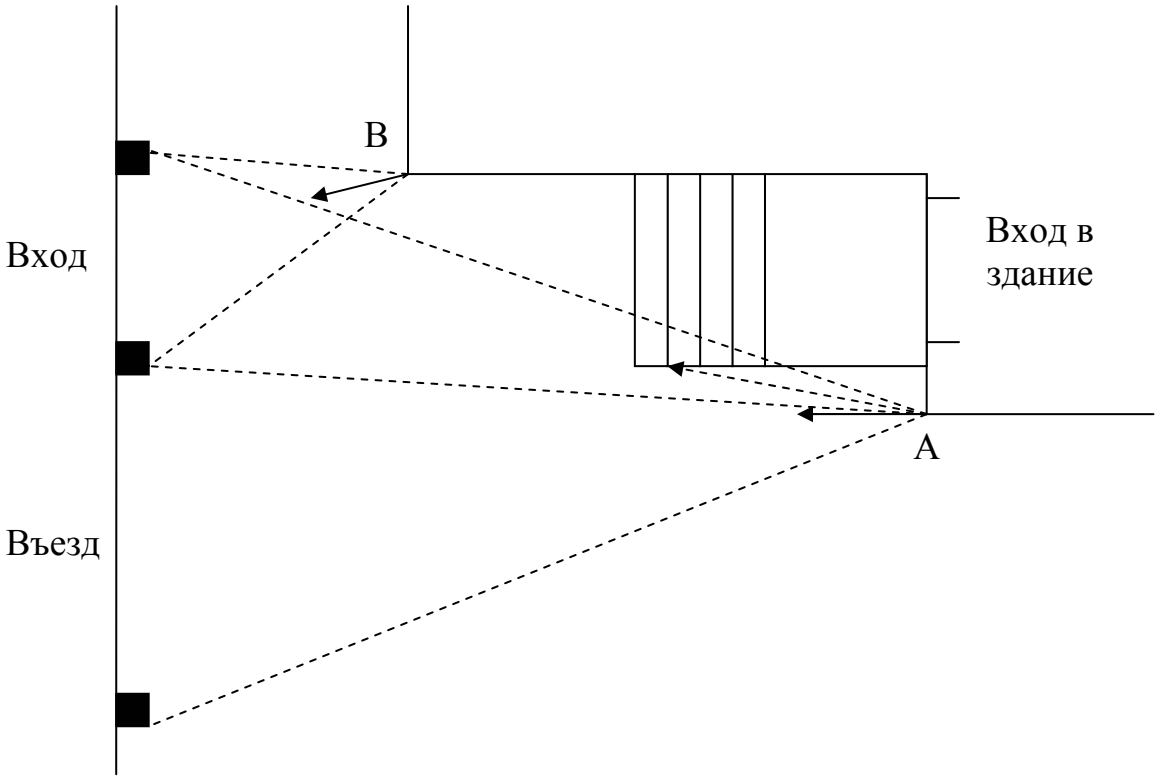

Рис. 2.7. Наблюдение за входом и подъездом.

Выбор места монтажа камер для наблюдения за автозаправочной станцией и станцией автосервиса представлен на рис. 2.8.

Критическими зонами для установок такого рода являются выезд от бензозаправочной колонки, так же как и площадка для демонстрации товаров внутри помещения магазина и кассового помещения. Кроме того, оказывается рациональным и наблюдение за подъездом к моечной установке.

Рис. 2.8 показывает типичное расположение видеокамер в установках такого рода, т.к. наружные камеры К1-К3 специально ориентированы на распознавание номерных знаков подъезжающих автомашин, на них должны ставиться только объективы с малым горизонтальным углом обзора (в зависимости от условий еще меньше, чем показано на примере). То же самое рекомендуется и на подъезде к моечной установке.

С помощью записи на видеомагнитофон, который осуществляет длительную временную запись, в сочетании с мультиплексором можно восстановить, какие автомобили покинули бензоколонку без оплаты.

Для внутренних зон магазина остаются в силе рекомендации, изложенные выше на примере супермаркета. Устанавливается такой угол обзора камер, ко-

торый предоставляет возможность оптимального просмотра критических зон.

Выбор места монтажа камер для наблюдения за подверженным угрозе участком ограды на промышленном предприятии представлен на рис. 2.9.

При наблюдении за оградой ни в коем случае не должны быть применены камер на дистанционно управляемых головках с изменяемой пространственной ориентацией, к примеру, с целью свести до минимума число установленных для этого вида работы камер. Потенциальный преступник мог бы при этом согласовать свою активизацию с соответствующим направлением камеры и таким образом остаться необнаруженным.

При наблюдении с помощью жестко установленных камер длина участка ограды, попадающего в поле зрения одной камеры, должна составлять не более 50 м.

При выборе мест монтажа камер в наружной зоне необходимо принять во внимание, что по возможности в середину поля зрения камеры не должны попадать объекты с большими отражающими площадями.

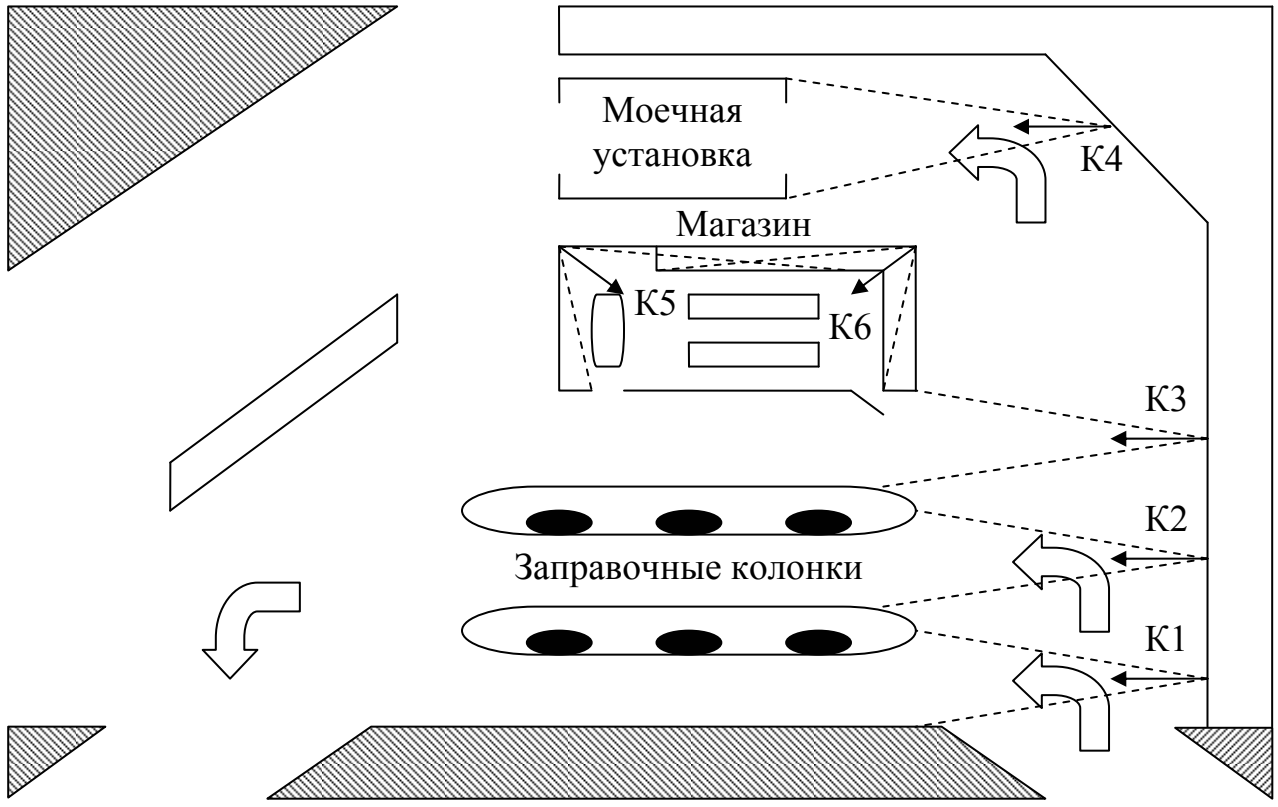

Рис. 2.8. Наблюдение за автозаправочной станцией и станцией автосервиса.

В любом случае при наблюдении за открытым участком местности обязательно должен быть исключен из поля зрения камеры прямой и отраженный солнечный свет, что демонстрируется на рис. 2.10. При открытом горизонте должно быть также вычислено наиболее низкое расположение солнца в зимние месяцы. В этом случае часто подходящим решением является выбор более высокого места монтажа камеры.

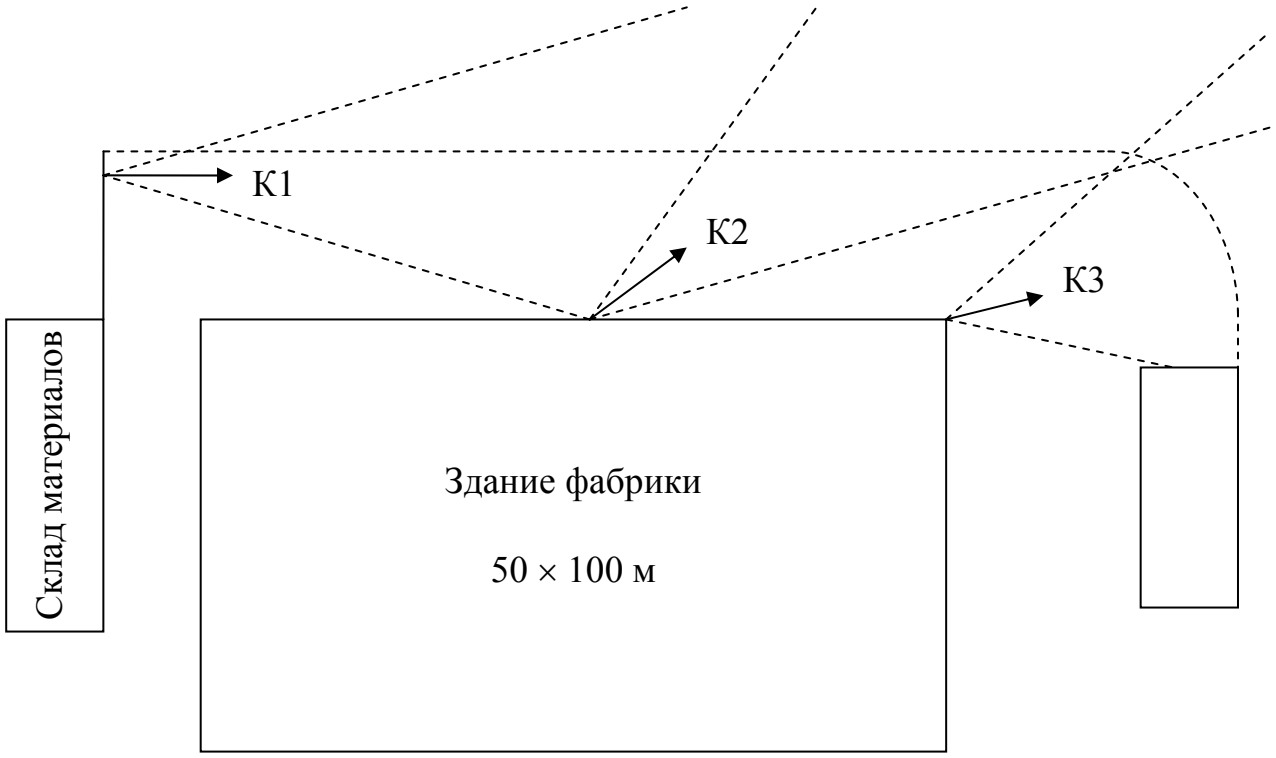

Рис. 2.9. Наблюдение за подверженным угрозе участком ограды.

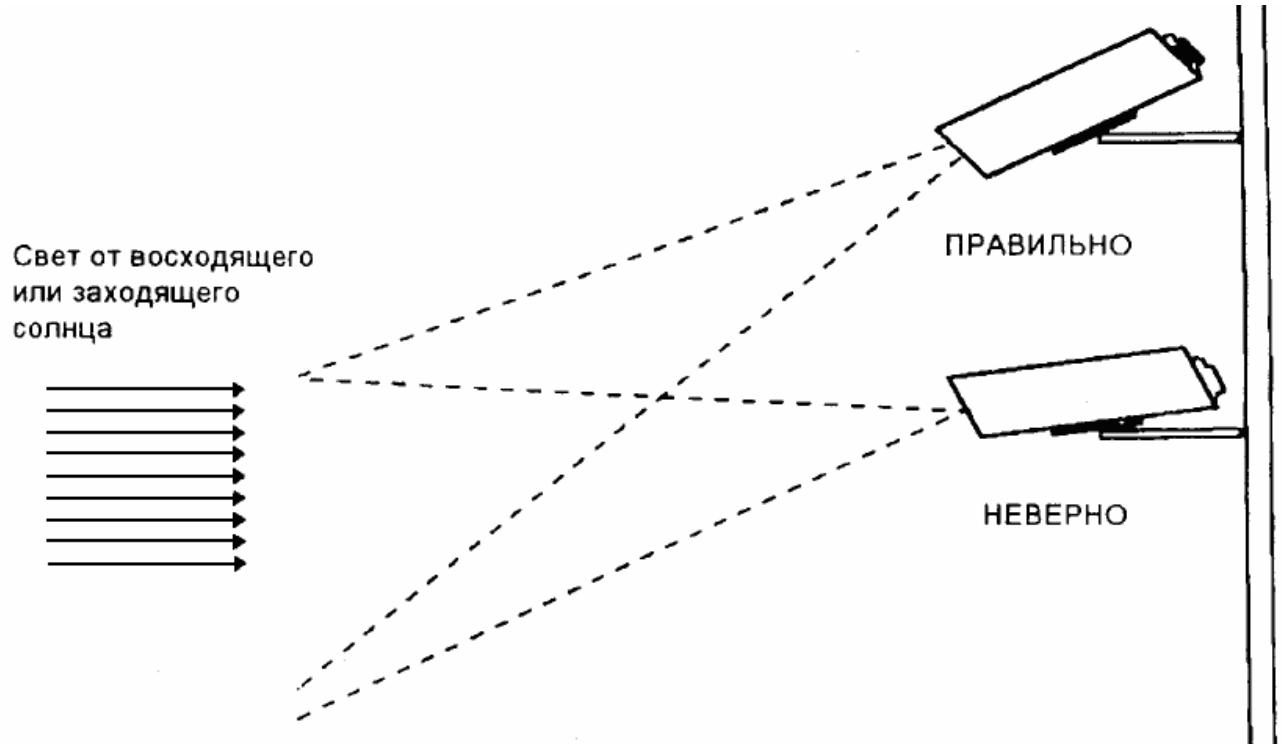

Рис. 2.10. Выбор правильного места монтажа камеры.

В большинстве случаев имеется возможность укрепить наружные камеры на стене здания или другого строения. Промышленность предоставляет для это-

го соответствующую монтажную арматуру, подходящую также для применения дистанционно управляемых головок с изменяемой пространственной ориентацией. В любом случае вся используемая для наружного применения монтажная арматура изготавливается из высококачественной стали и имеет высокую коррозионную стойкость.

2.3. Контрольные вопросы

1. В каком виде наиболее часто выполняются современные телевизионные установки?

2. Какие основные блоки входят в состав структурной схемы системной видеотехники?

3. Какие возможности и преимущества самостоятельно или в сочетании с другой техникой предоставляют видеосистемы наблюдения?

4. В каких случаях на объектах применяются видеосистемы?

5. В чём заключается рационализация применения видеосистем?

6. Для каких целей в измерительной технике применяются видеосистемы?

7. Как могут использоваться видеосистемы в науке и медицине?

8. Что является важнейшим шагом в разработке концепции видеосистемы?

9. Какая существует классификация видеоустановок по их типам?

10. Что показывает схема проектирования видеоустановки, составленная компанией Philips CSS?

11. В чём заключается суть подхода, который справедлив для всех случаев внутреннего применения видеокамер?

12. Какие примеры внутреннего монтажа видеокамер вам известны?

13. Какие примеры наружного монтажа видеокамер вам известны?

14. Что в обязательном порядке необходимо принять во внимание при выборе мест монтажа видеокамер в наружной зоне?

2.4. Задание

1. Изучить содержание файла «Основы работы в VideoCAD», а также справку для программы проектирования телевизионных систем VideoCAD.

2. Получить у преподавателя план объекта.

3. С помощью программы VideoCAD спроектировать систему видеонаблюдения для полученного плана объекта согласно рекомендациям по проектированию, приведённых в пункте 2.2.2. Высоту потолка проектируемого помещения принять равной 2,5 м.

4. Показать выполнение лабораторной работы преподавателю.

2.5. Содержание отчета

1. Цель работы.

2. Распечатка размещения видеокамер на плане объекта в горизонтальной проекции из программы VideoCAD.

3. Схема размещения оборудования разработанной системы видеонаблюдения. Пример оформления схемы размещения представлен в приложении А на рис. А.2.

4. Конкретные предложения по снижению затрат на проектирование и монтаж удобной архитектуры системы видеонаблюдения в соответствии с планом выбранного объекта.

5. Выводы по работе.

ЛАБОРАТОРНАЯ РАБОТА №3
ПРОЕКТИРОВАНИЕ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

3.1. Цель работы

Изучить теоретические основы проектирования систем контроля и управления доступом и получить практические навыки проектирования данных систем с использованием программы StilPost.

3.2. Теоретические сведения

Электронные системы контроля доступа (СКД) начали широко применяться в технических системах безопасности с 80-х годов XX века, в связи с развитием микропроцессорной технологии.

СКД прошли длительный эволюционный путь от простейших кодовых устройств, управляющих дверным замком, до сложных компьютерных систем, охватывающих целые комплексы зданий. Большинство современных предприятий и учреждений, как государственных, так и частных, имеют собственные электронные системы контроля доступа.

В настоящее время на отечественном рынке технических средств охраны предлагается широкий ассортимент оборудования для систем контроля доступа различной степени сложности. Однако даже самые совершенные приборы сами по себе не могут обеспечить должной защиты, если не работает человеческий фактор – дисциплинированность, профессионализм, ответственность службы безопасности и сотрудников организации.

Далее будет рассмотрена теория построения системы контроля доступа и назначение работающих в ней технических средств охраны.

3.3. Методика построения охранной системы контроля доступа

Априори считается, что система контроля и управления доступом (СКУД) является третьим рубежом защиты после систем охранно-пожарной сигнализации и видеонаблюдения, но ни в коем случае не заменяет бдительных сотрудников службы безопасности и не исключает необходимость закрывать двери. Хотя бы потому, что основная задача системы контроля доступа – регламентировать передвижение сотрудников и посетителей в рабочее время и предотвращать попадание нежданных гостей в охраняемые помещения.

Несмотря на уникальность каждой конкретной системы контроля доступа, есть и будут существовать «три кита», без которых ограничение доступа попросту невозможно:

– управляющие контроллеры;

– устройства идентификации личности;

– оборудование ограничения доступа.

Далее будут вкратце описаны принципы работы названных элементов, включая достоинства и недостатки наиболее распространенных из них.

3.3.1. Основные характеристики СКД

Система контроля доступа – совокупность программно-технических средств и организационно-методических мероприятий, с помощью которых решается задача контроля и управления посещением отдельных помещений, а также задача оперативного контроля за персоналом и временем его нахождения на территории объекта.

Использование в качестве пропускной системы предприятия СКД позволяет:

– контролировать доступ людей в служебные помещения;

– контролировать доступ автомобильного транспорта на территорию объекта;

– организовать базы данных на каждого работника или посетителя;

– отслеживать процесс прохождения сотрудниками точек контроля;

– организовать учет рабочего времени персонала.

Всем сотрудникам компании, в которой установлена СКД, выдаются специальные электронные пропуска, представляющие собой пластиковые карты или брелоки, которые содержат персональные коды доступа. Считыватели, устанавливаемые у входа в контролируемое помещение, распознают код идентификаторов. Информация поступает в СКД, которая на основании анализа данных о владельце идентификатора, принимает решение о разрешении допуска или запрете прохода того или иного сотрудника на охраняемую территорию. База данных позволяет оперативно разыскать сотрудника на территории по последней точке прохода, где он предъявлял идентификатор.

В каждой точке прохода может быть несколько тайм зон (временных ограничений на доступ). Например, сотруднику разрешается проход только в интервале времени $10^{\underline{00}} – 17^{\underline{00}}$.

В качестве исполнительных устройств СКД могут использоваться электромеханические или электромагнитные замки различных типов, турникеты, автоматические двери и т.п. Объектом доступа может быть не только человек, но и автомобиль, с закрепленным на нем специальным устройством. Исполнительными механизмами СКД в этом случае являются шлагбаумы и автоматические привода ворот.

Основными характеристиками системы контроля доступа являются:

– контроль и регистрация прохода сотрудников в разрешенное время или в соответствии с допуском в охраняемые помещения;

– ведение архива проходов;

– отображение состояния системы в режиме реального времени на дисплее компьютера;

– автоматический учет рабочего времени;

– сравнение фотографии сотрудника, хранящейся в базе данных, с реальным изображением с видеокамеры зоны прохода;

– составления отчетов по параметрам: вход / выход, тревоги, дежурств, рабочего времени и пр.

– фотографирование сотрудников и посетителей с сохранением фотографий в картотеке.

3.3.2. Компоненты СКД

3.3.2.1. Управляющий контролер. Контроллер СКД – это устройство, опрашивающее считыватели и управляющее замком или турникетом. Все контроллеры СКД объединяются в общую сеть, где каждый имеет свой уникальный адрес. Центральное устройство (обычно персональный компьютер), имеет возможность обращаться к каждому контроллеру, используя его адрес и специальную систему команд. В современных СКД предусмотрена возможность удаленного контроля, то есть доступа к данным с другого компьютера через сеть. Удаленный компьютер (клиент) может иметь полный доступ к данным сервера СКД, причем информация на нем динамически обновляется по мере того, как происходят те или иные события.

Каждое событие доступа, будь то предъявление идентификатора или нажатие кнопки запроса на выход, фиксируется контролером СКД. В случае разрешения допуска, контролер системы приводит в действие исполнительные устройства, такие как электромагнитные замки, турникеты, автоматические шлагбаумы, электроприводы ворот. В противном случае исполнительные устройства блокируются, включается сигнализация и оповещается охрана. В СКД предусмотрены различные возможности для предоставления доступа людей в помещения: групповой и индивидуальный доступ, круглосуточный доступ и доступ по расписанию, постоянный доступ и доступ на определенный период. Контроллер может иметь входы для охранных шлейфов, выход управления сиреной, кнопку запроса на выход и кнопку аварийного выхода. Эти кнопки необходимы для возможности выхода при утере идентификатора и выхода в случае пожара. Функция контроля входа / выхода служит для контроля присутствия сотрудников на рабочих местах. Программное обеспечение контролера СКД позволяет составлять ежедневный отчет, куда можно включать периоды отсутствия сотрудников в течение рабочего дня.

Любой контроллер СКД, в принципе, состоит из четырёх основных частей, представленных на рис. 3.1.

Принцип работы и взаимодействия этих частей контроллера можно пояснить на простом примере: человек подходит к заградительному механизму (например, к закрытой двери) и для того, чтобы получить доступ на защищаемую территорию предъявляет собственный идентификатор (например, proximity карту) системе контроля доступа, что иллюстрируется на рис. 3.2.

Рис. 3.1. Структурная схема контроллера СКД.

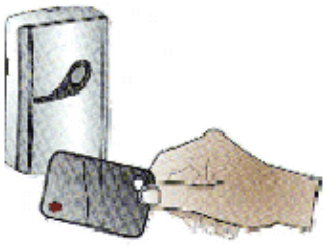

Рис. 3.2. Предъявление идентификатора.

Считыватель карт передает предложенную информацию на схему обработки сигналов контроллера. Далее информация в цифровом виде выдается на схему принятия решения, которая заносит факт попытки прохода в схему буфера событий, запрашивает схему базы данных на предмет правомочности прохода и, в случае положительного ответа, приводит в действие исполнительное устройство (например, электромагнитный замок). Ограничение уже снято, но система контроля доступа ещё не завершила обработку информации: сам факт прохода именно этого человека заносится в схему буфера событий.

В зависимости от мощности системы контроля доступа различные контроллеры, естественно, разделяются по емкости базы данных и буфера событий. Как правило, схема базы данных является энергонезависимой, то есть записывается от собственного источника. Возможны также различия по максимальному числу обслуживаемых устройств идентификации.

Большинство современных СКД имеют удобный графический оконный интерфейс и предоставляют возможность гибкой настройки для конкретной конфигурации оборудования.

3.3.2.2. Считыватели системы контроля доступа. Считыватель представляет собой устройство, которое позволяет считывать информацию, записанную на идентификаторе. Эту информацию он передает на контролер, который принимает решение о допуске человека в помещение. Устройства СКД позволяют

распознавать персональный код доступа при поднесении идентификатора к считывателю. Наиболее удобной является бесконтактная технология Proximity – она обеспечивает считывание кодовой информации через такие материалы, как одежда, сумки, кошельки и даже стены. Высокая помехоустойчивость обеспечивает надежную работу устройств системы контроля доступа, исключая влияние брелоков, ключей, зажигалок и прочих предметов, на передачу кода с идентификатора.

3.3.2.3. Идентификатор системы контроля доступа. В качестве идентификатора системы контроля доступа могут применяться:

– код доступа, набранный на кнопочной клавиатуре;
– считыватели магнитных карт;
– считыватели бесконтактных Smart-карт (интерфейс Wegand);
– считыватели Proximity карт;
– считыватели ключа Touch-Memory;
– считыватели штрих-кодов;
– биометрические считыватели.

Наиболее распространенными идентификаторами являются: бесконтактная карточка (Proximity карты / брелоки), пластиковая карточка с магнитным носителем кода или таблетка типа Touch-Memory. Один и тот же идентификатор может открывать как одну дверь, так и служить «ключом» для нескольких дверей. Для временных сотрудников и посетителей оформляются временные или разовые «пропуска» – карточки с ограниченным сроком действия.

Бесконтактные радиочастотные Proximity карты / брелоки – наиболее перспективный в данный момент тип карт. Бесконтактные карточки срабатывают на расстоянии и не требуют четкого позиционирования, что обеспечивает их устойчивую работу, удобство использования и высокую пропускную способность.

Магнитные карты – наиболее широко распространенный вариант. Код записывается на магнитную полосу карты, для его распознания необходимо провести картой внутри считывателя.

Touch-Memory – металлическая таблетка, внутри которой расположен микрочип. При касании таблетки считывателя, из памяти таблетки в контроллер пересылается уникальный код идентификатора.

Стоит отметить, что в настоящий момент считыватели штрих-кодов практически не устанавливаются в СКД, поскольку подделать пропуск чрезвычайно просто на принтере или на копировальном аппарате.

3.3.2.4. Замки СКД. Современные СКД комплектуются в основном электромагнитными замками. Их основное преимущество в отсутствии движущихся частей и исключительной износоустойчивости. Удержание двери осуществляется создаваемым замком магнитным полем с силой до 500 кг. При этом потребление энергии минимальное, а эффективность выше всяких ожиданий.

3.3.2.5. Турникеты СКД. Наиболее часто в СКД применяется электромеханический турникет-трипод. Данный турникет используется в тех случаях, когда необходимо обеспечить контроль однократных проходов при высокой пропускной способности, и имеет следующие отличительные особенности:

– компактность и изящный внешний вид;
– простота монтажа и установки;
– управление при помощи кнопочного пульта и / или СКД.

3.3.2.6. Ограждения СКД. Ограждения предназначены для формирования необходимых зон доступа и коридоров прохода людей. Ограждения могут устанавливаться как дополнение к турникетам, так и как самостоятельные элементы СКД.

К системам ограждениям также принято относить автоматические шлагбаумы и автоматику для открытия и закрытия ворот.

Обобщённая структурная схема СКУД представлена на рис 3.3.

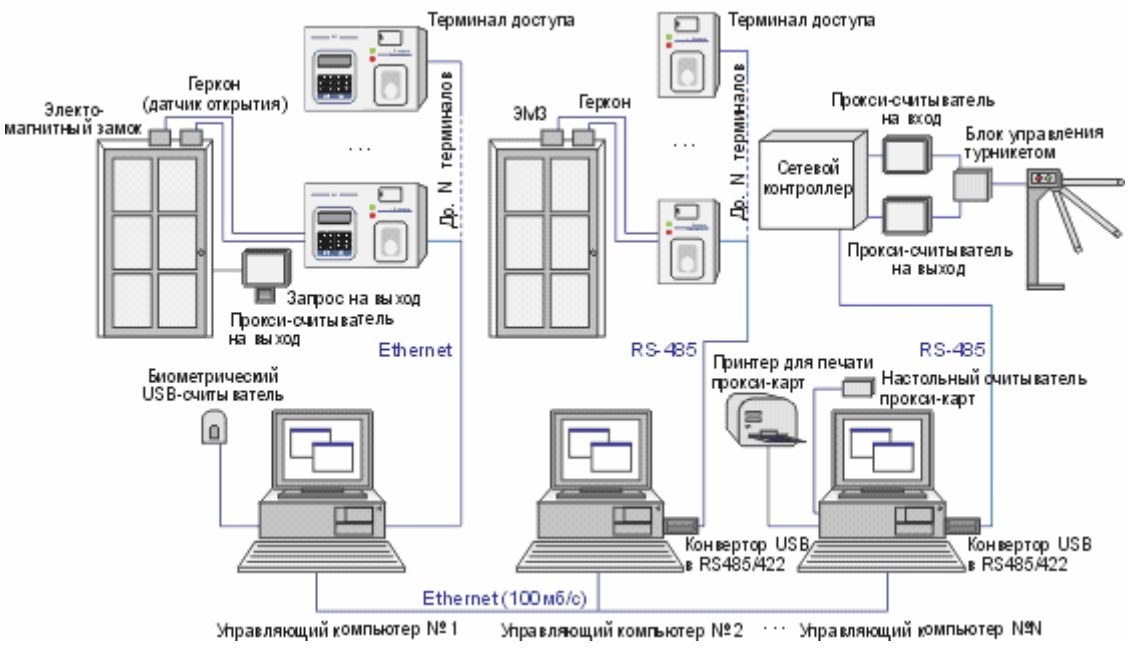

Рис. 3.3. Обобщённая структурная схема СКУД.

3.4. Программное обеспечение StilPost

Программное обеспечение StilPost™ разработано компанией StilSoft© для работы с аппаратными устройствами, которые применяются в СКД. Данное программное обеспечение обеспечивает простой и в то же время мощный интерфейс, позволяющий системным администраторам и другим пользователям управлять СКУД с непринужденной гибкостью.

3.4.1. Основные принципы построения системы

• StilPost состоит из управляющих компьютеров с программным обеспечением, контроллеров СКУД, устройств идентификации и устройств ограничения доступа.

• Устройства идентификации и устройства ограничения доступа могут подключаться как напрямую к управляющим компьютерам, так и через контроллеры СКУД.

• StilPost имеет центральную базу данных, в которых хранятся все правила доступа, пользователи и события происшедшие в системе. Любой узел системы может содержать локальную копию базы данных и благодаря этому иметь возможность полнофункционально работать автономно неограниченное время.

• В качестве управляющего компьютера может выступать любой компьютер, имеющийся на предприятии Работа системы абсолютно незаметна для пользователя данного компьютера.

• StilPost поддерживает несколько марок автономных контроллеров и интерфейсных модулей различных производителей. Все эти контроллеры можно использовать совместно.

• StilPost работает с широким перечнем разнообразных устройств идентификации производимых в настоящее время, в том числе считыватели отпечатка пальца.

3.4.2. Функциональные возможности

– создания зон допуска с произвольным уровнем вложенности;

– раздельные взаимозаменяемые графики допуска и учета рабочего времени;

– доскональная проработка функциональных возможностей предприятия, не имеющего стабильных графиков доступа;

– удобная работа с больничными, отпусками, праздничными днями;

– параллельная работа всех модулей позволяет менять правила работы системы практически на лету;

– распределенная трехзвенная клиент-серверная архитектура позволяет использовать совместно базы данных различных типов;

– система генерации отчетов удовлетворит самого взыскательного пользователя;

– гибкие правила для создания постоянных, временных и разовых пропусков;

– удобный редактор пропусков;

– возможность выдачи одному человеку ряда пропусков на различных носителях;

– осуществление «запрета повторного прохода в одну и ту же зону»;

– невозможность использования пропуска без фактического прохода человека;

– удаленный мониторинг деятельности системы, контроль за сотрудниками службы безопасности;

– возможно одновременное администрирование системы большим количеством человек;

– резервное копирование баз данных, реплицирование части баз данных на узлы системы как средство повышения «живучести» информационного хранилища;

– проверка целостности и семантической достоверности информации, содержащейся в базе.

3.4.3. Программные модули

Любой программный модуль может размещаться на любом компьютере в сети предприятия. При размещении нескольких модулей на одном компьютере, все компоненты работают в едином интерфейсе. Устройства идентификации, ограничения доступа, контроллеры СКУД могут подключаться к компьютеру, на котором установлен модуль «StilPost™: Сервис обслуживания устройств». Модуль «StilPost™ Управление системой» имеет в своем составе модуль «StilPost™: Сервис обслуживания устройств». Минимально возможный набор модулей – «StilPost™: Управление системой» и «StilPost™: Бюро пропусков».

«StilPost™: Управление системой» - используется для первоначальной настройки оборудования системы StilPost, управления пользователями системы, включает сервис обслуживания устройств.

«StilPost™: Проходная» – модуль контроля легитимности прохода с фотоидентификацией. Позволяет обслуживать до 8 проходных одновременно. В комплексе с системой видеонаблюдения «Видеолокатор™» позволяет производить фотоидентификацию удаленно.

«StilPost™: Мониторинг событий» – модуль, позволяющий отслеживать все события, происходящие в системе и выдавать отчеты.

«StilPost™: Учет рабочего времени» – модуль учета рабочего времени.

«StilPost™: Бюро пропусков» – Предназначен для занесения информации о пользователях системы, выдачи и учета пропусков, ведения графиков доступа.

«StilPost™: Контрольно-пропускной пункт» – модуль контроля легитимности проезда через контрольно-пропускной пункт с фотоидентификацией. В комплексе с системой видеонаблюдения «Видеолокатор™» позволяет производить фотоидентификацию удаленно. Может быть оснащен модулем распознавания автомобильных номеров. Реализация некоторых возможностей требует интеграции с системой видеонаблюдения «Видеолокатор™».

«StilPost™: Сервис обслуживания устройств» – Обеспечивает обмен данными между устройствами идентификации и ядром системы, управляет устройствами ограничения доступа. Выполнен в виде сервиса операционной системы,

автоматически загружается при её старте. Абсолютно незаметен для пользователя компьютера, потребляет очень мало системных ресурсов. Данный модуль применяется при построении распределенных систем контроля доступа, когда устройства ограничения доступа и идентификации физически подключаются к разным компьютерам, соединенным между собой локальной сетью или через Интернет. Не поддерживает сканер отпечатка пальца.

«StilPost™: Сервис обслуживания устройств с поддержкой биометрической аутентификации» – Обеспечивает обмен данными между устройствами аутентификации и ядром системы. Управляет устройствами ограничения доступа. Позволяет подключать сканеры отпечатка пальца STS-710. Выполнен в виде сервиса операционной системы. Автоматически загружается при старте системы. Абсолютно незаметен для пользователя компьютера, потребляет очень мало системных ресурсов. Данный модуль применяется при построении распределенных систем контроля доступа, когда устройства ограничения доступа и идентификации физически подключаются к разным компьютерам, соединенным между собой локальной сетью или через Интернет.

«StilPost™: Биометрическая аутентификация» – Модуль распознавания отпечатков пальца. Позволяет организовать аутентификацию человека по отпечатку пальца. Применение считывателей отпечатка пальца STS-710 позволяет существенно повысить уровень безопасности и надежности системы контроля и управления доступом. Модуль интеграции с 1С Бухгалтерией позволяет загружать из программы 1С Бухгалтерия анкетные данные сотрудника, его фотографию, информацию о больничных листах и отпусках, другую необходимую информацию. Может быть настроен для выгрузки из системы «StilPost» в 1С Бухгалтерию табеля учета рабочего времени.

«StilPost™: Распознавание документов» – Модуль «StilPost™: Распознавания документов» предназначен для автоматизации процесса ввода и обработки формализованных документов (паспортов, водительских удостоверений и др.), построенных по стандартизованной форме и напечатанных на гербовой бумаге. Система обеспечивает автоматизированный ввод документов, распознавание текстовой и графической информации, редактирование сомнительно распознанных полей и преобразование считанной информации в согласованный формат экспорта-импорта документов.

3.4.4. Быстрый старт

Рассмотрим шаги, которые нужно предпринять для минимальной первоначальной настройки системы:

1. Установите программное обеспечение системы StilPost. При использовании сервера баз данных Oracle, применяйте специальный инсталлятор СУБД, входящий в поставку. При использовании СУБД MSDE сервер баз данных установиться автоматически.

2. Настройте IP адрес компьютера, на котором находится сервер баз данных

в модуле «Настройка системы».

3. В модуле «Управление системой» на закладке «Зоны» добавьте хотя бы одну зону.

4. В модуле «Управление системой» на закладке «Проходные» добавьте проходную между зонами.

5. В модуле «Управление системой» на закладке «Компьютеры» добавьте физически подключенные устройства идентификации и ограничения доступа.

6. В модуле «Управление системой» на закладке «Проходные» назначьте правила работы виртуальных устройств при проходе через каждую добавленную проходную.

7. В модуле «Бюро пропусков» добавьте сотрудников, группы сотрудников. Добавьте сотрудникам пропуска и графики рабочего времени.

После этого система готова к работе.

3.4.5. Начало работы с программой

Для запуска StilPost на вашем компьютере, выполните следующую последовательность шагов:

1. Нажмите «Пуск» на панели управления, затем «Программы» → «StilSoft» → «StilPost» → «СтилПост™ 4.1.1 DEMO».

2. После появления системного диалогового окна входа в систему, представленного на рис. 3.4, имя пользователя и пароль оставьте без изменения и нажмите <OK>.

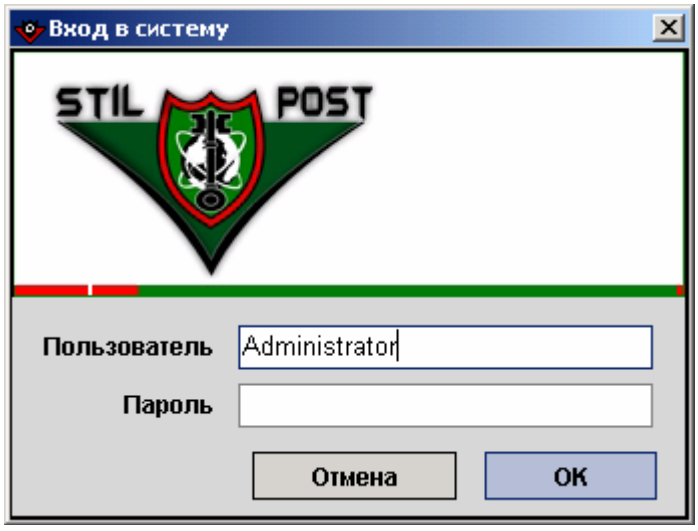

Рис. 3.4. Диалоговое окно входа в систему.

Примечание: т.к. программа StilPost используется исключительно в учебных целях, не в коем случае не меняйте имя пользователя и пароль при даль-

нейшей работе с программой для избегания случаев невозможности войти в систему другими пользователями!

3.4.6. Интерфейс программы

На рис. 3.5 показан главный пользовательский интерфейс.

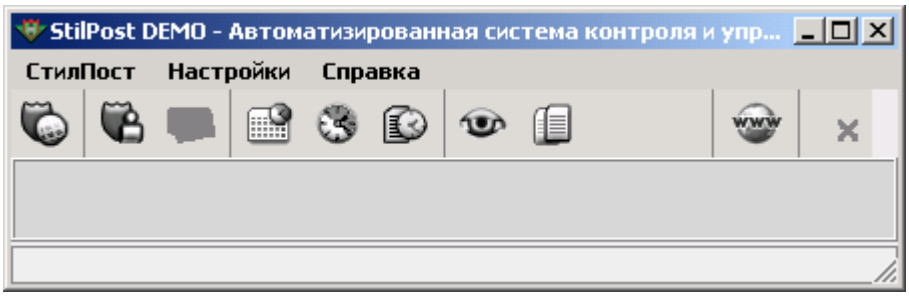

Рис. 3.5. Главный пользовательский интерфейс.

В верхней части главного окна программы располагаются меню «СтилПост», «Настройки» и «Справка». Меню «СтилПост» содержит следующие режимы:

– Управление системой. С помощью данного режима можно произвести настройку оборудования системы, добавить проходные, а также зоны контроля доступа.

– Управление авторизацией. Данный режим позволяет добавлять и удалять пользователей из системы, назначать права пользователям и группам пользователей.

– Дизайнер пропусков. С помощью данного режима можно создавать шаблоны пропусков.

– Бюро пропусков. В данном режиме можно добавлять пользователей, формировать и выдавать им пропуска, создавать группы пользователей, добавлять пользователей в определенные группы, а также добавлять графики контроля доступа, разграничивающие доступ в определённые зоны, определенным группам сотрудников.

– Графики. С помощью данного режима можно создавать, редактировать и удалять графики сотрудников.

– Учет рабочего времени. В данном режиме можно добавлять группам сотрудников графики рабочего времени.

– Увольнительные, отпуска. Данный режим позволяет вводить отгулы, увольнительные, отпуска, больничные листы сотрудников, для последующего использования в табелях рабочего времени.

– Праздничные дни. В данном режиме можно занести информацию о праздничных днях и о перенесённых рабочих днях.

– Учет рабочего времени – отчеты. Режим позволяет выводить на печать

отчеты о посещаемости сотрудников и табеля рабочего времени.

– Проходная. С помощью данного режима можно просмотреть информацию о сотрудниках, которые проходят через проходные в реальном времени.

– Мониторинг и отчеты. В данном режиме можно отслеживать посещения сотрудников.

– План. В данном режиме отображается план системы StilPost вашего объекта, где можно просмотреть, все ли устройства работают, есть ли неполадки в системе. А также управлять отдельно каждой проходной и камерой.

– Настройка. В данном режиме можно произвести настройку системы.

Ниже кнопок меню располагаются кнопки – режимы программы: «Управление системой», «Бюро пропусков», «Графики», «Учет рабочего времени – отчеты», «Проходная», «Мониторинг и отчеты».

С помощью меню «Справка» можно вывести интерактивную справку по программе.

3.5. Контрольные вопросы

1. Какова основная задача СКД?
2. На каких «трёх китах» базируются современные СКУД?
3. Какое определение наиболее полно определяет СКД с точки зрения выполняемых ею задач?
4. Что позволяет использование СКД в качестве пропускной системы предприятия?
5. Какие характеристики являются основными для СКД?
6. Каково назначение управляющего контроллера в СКД?
7. Из каких четырёх основных частей состоит структурная схема контроллера СКД?
8. Как разделяются контроллеры в зависимости от мощности СКД?
9. Каково назначение считывателей в СКД?
10. Какие устройства могут применяться в качестве идентификатора системы контроля доступа?
11. Каково назначение электромагнитных замков в СКД?
12. Каково назначение турникета-трипода в СКД?
13. Каково назначение ограждений в СКД?
14. Какой вид имеет обобщённая структурная схема СКУД?

3.6. Задание

1. Изучить справку для программы проектирования СКУД StilPost.
2. Получить у преподавателя план объекта.

3. С помощью программы StilPost спроектировать СКУД для полученного плана объекта, используя все режимы работы системы, приведённые в пункте 3.4.6.

4. Показать выполнение лабораторной работы преподавателю.

3.7. Содержание отчета

1. Цель работы.

2. Распечатка созданной конфигурации СКУД из программы StilPost.

3. Схема размещения оборудования разработанной СКУД. Пример оформления схемы размещения представлен в приложении А на рис. А.3.

4. Конкретные предложения по снижению затрат на проектирование и монтаж удобной архитектуры СКУД в соответствии с планом выбранного объекта.

5. Выводы по работе.

ЛАБОРАТОРНАЯ РАБОТА №4
БИОМЕТРИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ

4.1. Цель работы

Изучить теоретические основы проектирования биометрических систем безопасности и получить практические навыки работы с такими системами с использованием программы Demo.exe, имитирующей систему допуска в помещение с голосовым замком.

4.2. Теоретические сведения

Благодаря высоким оперативно-техническим характеристикам биометрические средства защиты пользуются особым вниманием специалистов. Эти средства нашли применение, в основном, в государственных учреждениях, требующих наиболее высоких уровней защиты, в частности, в военных организациях, вычислительных и научных центрах, в банковских хранилищах и др.

На сегодняшний день структура мирового рынка биометрических средств и систем выглядела следующим образом (рис. 4.1).

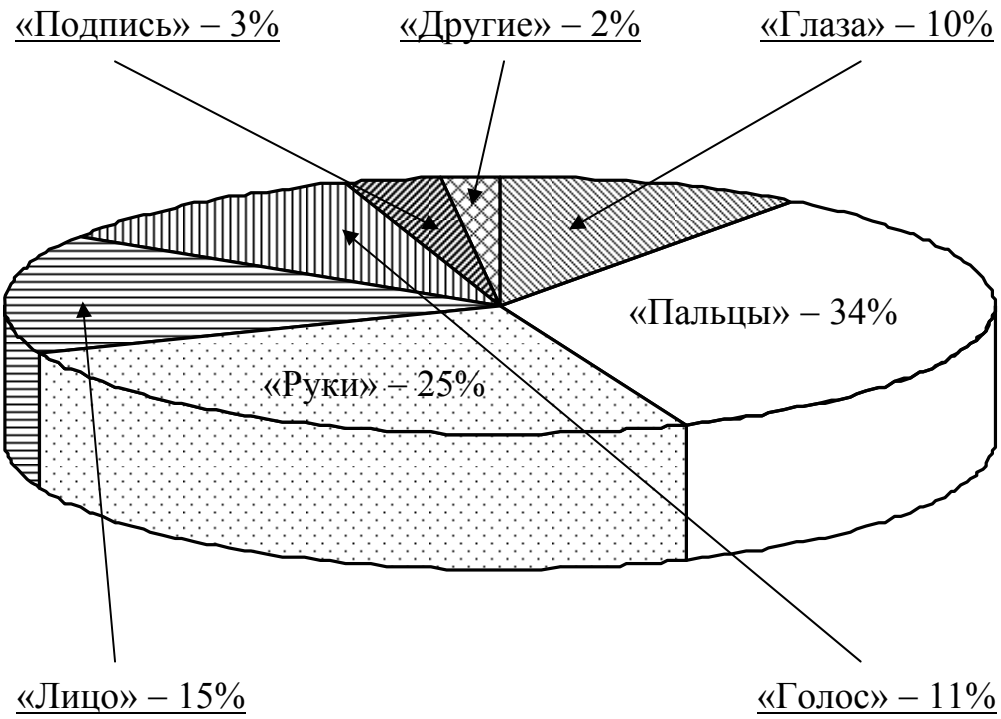

Рис. 4.1. Структура мирового рынка биометрических средств защиты.

Особое внимание привлекают к себе биометрические средства защиты информации (БСЗИ), что определяется их высокой надежностью идентификации и значительным прорывом в области снижения их стоимости.

В настоящее время отечественной промышленностью и рядом зарубежных фирм предлагается достаточно широкий набор различных средств контроля доступа к информации, в результате чего выбор оптимального их сочетания для применения в каждом конкретном случае вырастает в самостоятельную проблему. По конструктивным особенностям можно отметить системы, выполненные в виде моноблока, нескольких блоков и в виде приставок к компьютерам. Возможная классификация биометрических средств защиты информации, представленных на отечественном рынке, по биометрическим признакам, принципам действия и технологии реализации приведена на рис. 4.2.

Рис. 4.2. Классификация современных БСЗИ.

В настоящее время биометрические системы контроля доступа (БСКД) к информации завоевывают все большую популярность в банках, фирмах, связанных с обеспечением безопасности в телекоммуникационных сетях, в информационных отделах фирм и т. д. Расширение применения систем этого типа

можно объяснить как снижением их стоимости, так и повышением требований к уровню безопасности.

В число современных БСКД к информации входят подсистемы проверки по голосу, форме кисти руки, рисунку кожи пальцев, сетчатке или радужной оболочке глаза, фотографии лица, термограмме лица, динамике подписи, фрагментам генетического кода и др.

Все биометрические системы характеризуются высоким уровнем безопасности, прежде всего потому, что используемые в них данные не могут быть утеряны пользователем, похищены или скопированы. В силу своего принципа действия многие биометрические системы пока еще отличаются сравнительно малым быстродействием и низкой пропускной способностью. Тем не менее, они представляют собой единственное решение проблемы контроля доступа на особо важных объектах с малочисленным персоналом.

В настоящее время имеется большое количество алгоритмов и методов биометрической идентификации, отличающихся точностью, стоимостью реализации, удобством использования и т.п. Однако у всех биометрических технологий существуют общие подходы к решению задачи идентификации пользователя. Обобщенный алгоритм биометрической идентификации, характерный для всех известных БСЗИ, состоит из пяти этапов:

1. Сканирование объекта.
2. Извлечение индивидуальной информации.
3. Формирование шаблона.
4. Сохранение текущего шаблона с базой данных.
5. Выдача команды управления.

Как видно из представленного алгоритма биометрическая система распознавания устанавливает соответствие конкретных поведенческих или физиологических характеристик пользователя некоторому заранее заданному шаблону. Как правило, биометрическая система, реализующая этот обобщенный алгоритм, состоит их трех основных блоков и базы данных, представленных на рис. 4.3.

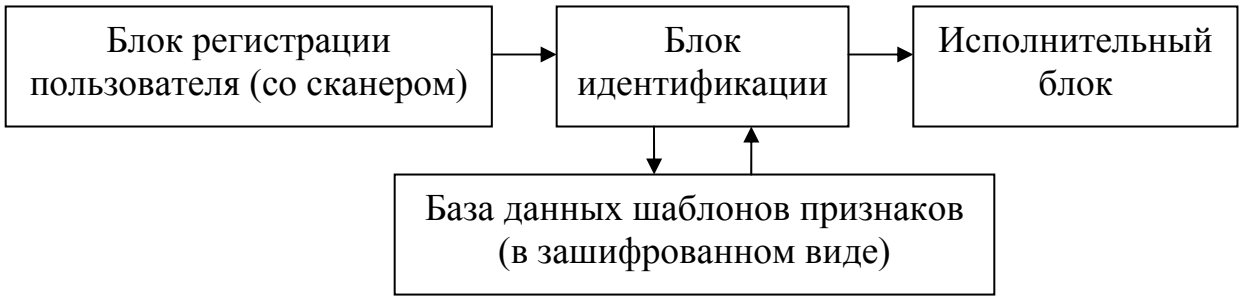

Рис. 4.3. Блок-схема типовой системы БСЗИ.

Большинство БСЗИ функционируют следующим образом: в базе данных системы хранится цифровой отпечаток пальца, радужной оболочки глаза или голоса. Человек, собирающийся получить доступ к охраняемому объекту, с по-

мощью микрофона, сканера отпечатков пальцев или других устройств вводит информацию о себе в систему. Поступившие данные сравниваются с образцом, хранимым в базе данных. Остановимся на некоторых из них.

4.2.1. Распознавание голоса

Распознавание голоса является технологий, которая позволяет пользователю применять свой голос в качестве устройства ввода данных. Распознавание голоса может использоваться для диктования текста компьютеру или для подачи команд компьютеру (например, для открытия программных приложений, развертывания меню или сохранения работы).

Более ранние системы распознавания голоса требуют отчетливого произношения каждого слова с заметными промежутками. Это позволяет машине определять, где заканчивается одно слово, и начинается следующее. Такие виды программ распознавания речи все еще применяются для управления компьютерными системами и работы с такими приложениями, как Web-браузеры или электронные таблицы.

Более современные приложения распознавания голоса позволяют пользователю бегло диктовать текст компьютеру. Такие новые приложения способны распознавать речь со скоростью до 160 слов в минуту. Приложения, которые позволяют распознавать непрерывный поток речи в основном предназначены для распознавания и форматирования текста, а не для управления самой компьютерной системой.

В технике распознавания речи используется нейронная сеть для «обучения» распознаванию человеческого голоса. В то время как вы говорите, программное обеспечение распознавания речи запоминает, каким образом вы произносите каждое слово. Такая индивидуализированная настройка позволяет производить распознавание голоса, несмотря на то, что у всех людей разное произношение и интонация.

Помимо «изучения» того, как вы произносите слова, системы распознавания голоса также используют грамматический контекст и частоту употребления отдельных слов для того, чтобы предугадать, какое слово вы желаете ввести. Такие мощные статистические средства позволяют программе найти в обширной языковой базе данных нужное слово до того, как вы его произнесете.

Биометрический подход, связанный с идентификацией голоса, характеризуется удобством в применении. Однако основным и определяющим недостатком этого подхода является низкая точность идентификации. Например, человек с простудой или ларингитом может испытывать трудности при использовании данных систем. В последнее время ведутся активные разработки по усовершенствованию и модификации голосовых систем идентификации личности, поиск новых подходов для характеристики человеческой речи, комбинации физиологических и поведенческих факторов. Сегодня идентификация по голосу используется для управления доступом в помещения средней степени секретности, например, лаборатории производственных компаний.

4.2.2. Распознавание по радужной оболочке глаза

Данный метод биометрической идентификации личности основывается на уникальных характерных признаках и особенностях радужной оболочки человеческого глаза. Радужная оболочка – это часть глаза, представляющая собой цветной круг, чаще всего коричневого или голубого цвета, окаймляющий черный зрачок. Процесс сканирования радужки начинается с фотографии. В специальном фотоаппарате, который обычно подносится очень близко к человеку, но не ближе 90 см, применяется инфракрасная подсветка для получения фото с очень высоким разрешением. На процесс фотографирования уходит всего от одной до двух секунд, затем полученное детальное изображение радужки преобразуется в схематическую форму, записывается и хранится для последующего сравнения / верификации. Очки и контактные линзы никак не влияют на качество изображения, а системы сканирования радужки проверяют живой глаз посредством измерения наблюдающихся в норме постоянных колебаний размера зрачка.

Внутренний край радужки определяется алгоритмом системы сканирования, который отображает в виде схемы индивидуальный рисунок и характерные особенности радужной оболочки. Алгоритм представляет собой серию указаний, которые направляют процесс интерпретации системой конкретной проблемы. Алгоритмы состоят из нескольких последовательных шагов и используются биометрической системой для определения соответствия между биометрическим образцом и зарегистрированными данными.

Радужная оболочка формируется еще до рождения человека, и, за исключением случаев повреждения глазного яблока, остается неизменной на протяжении всей жизни человека. Рисунок радужки является чрезвычайно сложным и несет в себе поразительно большой объем информации, а также имеет более 200 уникальных точек. Тот факт, что правый и левый глаз человека отличаются друг от друга, и что их рисунки очень легко зафиксировать в схематической форме, делает технологию сканирования радужной оболочки одним из самых надежных средств идентификации, не подверженным ложному сравнению и фальсификации.

Частота ложного распознавания в системах идентификации по радужке равна 1 к 1,2 миллионам, статистически это намного выше, чем результаты, демонстрируемые в среднем системами распознавания по отпечаткам пальцев. Реальным преимуществом является частота непризнания – количество действительных зарегистрированных пользователей, личность которых не распознается. Сканеры отпечатков пальцев допускают ошибки непризнания в 3% случаев, в то время как системы сканирования радужной оболочки отличаются частотой непризнания 0%.

Метод сканирования радужной оболочки начали применять и в аэропортах для таких разнообразных функций, как идентификация / верификация работников для прохождения через зоны ограниченного доступа, а также для идентификации пассажиров, наиболее часто пользующихся услугами авиакомпании

для быстрого прохождения ими паспортного контроля. Среди других сфер применения можно назвать переводы заключенных внутри тюрем, а также выпуск на свободу, помимо этого, следует перечислить такие проекты, как верификация при онлайновых покупках, онлайновом пользовании банковскими услугами, онлайновом голосовании и онлайновой торговле акциями. Метод идентификации по радужной оболочке обеспечивает высокий уровень безопасности пользователя, защиту частной информации, а также просто помогает поддерживать спокойствие и хорошее настроение клиента.

4.2.3. Сканирование геометрии кисти руки

В данном биометрическом методе для идентификации личности используется геометрическая форма кисти руки. Так как человеческие руки не являются уникальными, то необходимо сочетать несколько специфических характеристик для обеспечения динамической верификации. Некоторые сканирующие устройства измеряют только два пальца, другие измеряют полностью всю руку. Измеряемые характеристики включают изгибы пальцев, толщину и длину; толщину и ширину тыльной стороны руки; расстояние между суставами и общую структуру кости.

Следует отметить, что хотя структура кости и суставы являются относительно постоянными признаками, такие воздействия, как распухание тканей или ушибы могут исказить исходную структуру руки. Это может привести к ложному сопоставлению, тем не менее, количество приемлемых отличающих совпадений может быть отрегулировано в соответствии с потребностями определенного уровня обеспечения безопасности.

Для регистрации в системе сканирования, рука помещается на ровную поверхность, на которой предусмотрено считывающее устройство. Позиция руки фиксируется с помощью пяти штифтов, которые помогают правильно расположить руку в отношении фотокамер. Последовательность фотокамер создает трехмерные изображения боковых сторон и тыльной стороны руки. Сканирование руки является простым и быстрым процессом. Устройство сканирования может обработать трехмерные изображения за 5 или менее секунд, а верификация занимает не более 1 секунды. Программное обеспечение и аппаратные средства по захвату и верификации изображений могут быть легко интегрированы в составе автономных устройств. Те объекты, на которых имеется большое число точек доступа и пользователей, могут управляться централизованно, устраняя необходимость регистрации пользователя на каждом отдельном устройстве на всех точках доступа.

Во многих международных аэропортах уже используются приборы сканирования формы руки для того, чтобы позволить пассажирам, часто летающим на международных рейсах, не стоять в длинных очередях для прохождения различных иммиграционных и таможенных процедур.

На предприятиях сканирование руки используется для учета прихода / ухода и регистрации движения персонала, а также для общих процедур

учета рабочего времени. Это может иметь большое значение для устранения такой давней проблемы, как «отметка другом» времени прихода / ухода, а также других обманных действий.

4.2.4. Сканирование геометрии лица

Идентификация человека по чертам лица – одно из самых динамично развивающихся направлений в биометрической индустрии. Привлекательность данного метода основана на том, что он наиболее близок к тому, как люди обычно идентифицируют друг друга. Рост мультимедийных технологий, благодаря которым можно увидеть все больше видеокамер, установленных на городских улицах и площадях, аэропортах, вокзалах и других местах скопления людей, определили развитие этого направления.

Распознавание лица предусматривает выполнение любой из следующих функций: аутентификация – установление подлинности «один в один», идентификация – поиск соответствия «один из многих».

Основой любой системы распознавания лица является метод его кодирования. Стандартные математические методы кодирования основывается на том, что все лица могут быть получены из репрезентативной выборки лиц с использованием современных статистических приемов. Они охватывают пиксели изображения лица и универсально представляют лицевые формы. Фактически в наличии имеется намного больше элементов построения лица, чем количество самих частей лица. Однако оказывается, что синтезирование данного изображения лица с высокой точностью требует только малого числа (12-40) характерных элементов из полного доступного набора. Идентичность лица определяется не только характерными элементами, но и способом их геометрического объединения (т.е. учитываются их относительные позиции). Полученный сложный математический код индивидуальной идентичности – шаблон, который содержит информацию, отличающую лицо от миллионов других, и может быть составлен и сравнен с другими с феноменальной точностью. Шаблон не зависит от изменений в освещении, тона кожи, наличия / отсутствия очков, выражения лица, волос на лице и голове, устойчив к изменению в ракурсах.

4.2.5. Сочетание различных методов биометрической идентификации

Сканирование руки может легко сочетаться с другими биометрическими методами, например, с идентификацией по отпечаткам пальцев. Система, в которой относительно нечасто используется идентификация по отпечаткам пальцев, а сканирование руки производится часто, представляет собой двухуровневую структуру. Используемый часто компонент сканирования руки позволяет производить идентификацию личности с точностью 1:1 (один к одному), верифицируя, что пользователь действительно является тем, за кого он себя выдает. Компонент идентификации по отпечаткам пальцев, который используется менее часто, подтверждает личность пользователя и производит идентификацию с

точностью 1:N (один к множеству), т.е. сравнение производится с различными регистрационными данными.

4.2.6. Комбинированные биометрические системы

Комбинированная (мультимодальная) биометрическая система использует различные приложения для охвата различных типов биометрических данных. Это позволяет интегрировать два или более типа биометрического распознавания и верификационных систем для удовлетворения самых строгих требований к эффективности системы.

Мультимодальная система может, к примеру, включать комбинацию идентификации по отпечаткам пальцев, рисунку лица, голосу – плюс смарт-карта, или же любое другое сочетание биометрических характеристик. Такая усиленная структура использует все разнообразие биометрических данных человека и может использоваться там, где необходимо преодолеть ограничения какого-либо одного биометрического признака. Например, установлено, что 5% населения имеют неразличимые (нечеткие) отпечатки пальцев, голос может измениться от простуды, а распознавание по рисунку лица зависит от сильных изменений освещенности и позы объекта. Все эти недостатки могут быть преодолены в комбинированной системе, сочетающей заключения, сделанные на основе нескольких независимых друг от друга биометрических показателей. Мультимодальные системы в основном являются более надежными с точки зрения возможности фальсификации, так как труднее подделать целый ряд биометрических характеристик, чем фальсифицировать один биометрический признак.

Основными направлениями практического внедрения рассмотренных средств биометрического контроля доступа к информации в настоящее время являются:

– идентификация личности, паспортизация;

– электронная торговля;

– страхование;

– защита систем связи;

– общий контроль доступа к информационным объектам (мобильным и стационарным);

– контроль доступа в компьютерные и сетевые системы;

– контроль доступа в различные информационные хранилища, банки данных и др.

Последние разработки БСЗИ прекрасно взаимодействуют с новыми информационными технологиями, в частности, с сетевыми технологиями связи, такими как Интернет и сотовые системы связи. Анализ показывает, что современные возможности биометрических технологий уже сегодня обеспечивают необходимые требования по надежности идентификации, простоте использования и низкой стоимости средств идентификации пользователя.

4.3. Программное обеспечение Demo.exe, имитирующее СКД с голосовым замком

Программа Demo.exe, разработанная корпорацией AudiTech, имитирует простейший вариант системы допуска в помещение с голосовым замком и включает следующий набор файлов:

- Demo.exe – собственно сама программа.
- Audimic.exe – программа для настройки микрофона.
- Demo.psw – файл, содержащий параметрическое представление паролей пользователей (изменяется в процессе работы программы).
- Demo.cfg – текстовый файл конфигурации строк сообщений и звуков, используемых программой Demo.exe.
- Verify.dll – библиотека обработки речевого сигнала (БОРС).
- Protocol.log – текстовый файл, отражающий результат работы программы Demo.exe (изменяется в процессе работы программы).
- *.wav – несколько звуковых файлов в формате wav в соответствии с разделом [Sounds] файла Demo.cfg, предназначенных для звукового дублирования сообщений.

4.3.1. Описание библиотеки обработки речевого сигнала

БОРС представляет собой системно и аппаратно независимый комплекс программных средств параметризации оцифрованных РС. Модульная структура БОРС позволяет интегрировать её как в программы для компьютеров, работающие под различными операционными системами, так и в микроконтроллеры, включать и выключать вычисление отдельных параметров в зависимости от характера выполняемой задачи, быстродействия центрального процессора и объема памяти. В БОРС входят также модули поддержки различных аппаратных средств оцифровки звука. Для тех сред, где управление оцифровкой звука осуществляется посредством драйверов (Windows, OS/2) имеются модули, обеспечивающие интерфейс с этими драйверами. БОРС реализована как библиотека классов языка C++.

БОРС были разработаны с учётом следующих факторов:

– простота пользовательского интерфейса;

– защита от непреднамеренных ошибок использования объектов;

– возможность сохранения и считывания из файлов, что дает возможность поддерживать базы данных исходного речевого материала, а также базы данных признаков. Для нестандартных кодировок речевых сигналов предусмотрены виртуальные функции для приведения речевого сигнала к единой форме. Это дает возможность пользователю легко подстроить библиотеку под свои речевые базы данных или нестандартные устройства ввода (дельта-модуляция, мю-кодирование или любые другие методы);

– скорость вычислений (используются целочисленные методы обработки);

– легкость добавления новых методов анализа и обработки без модификации исходных текстов библиотеки;

– возможность строить базы данных признаков и собственно оцифрованную речь в файлах, как определенного формата, так и произвольного, задаваемого пользователем.

Основными параметрами и свойствами БОРС являются:

– частота дискретизации РС 8000, 10000, 11025, 16000 Гц;

– максимальная длина входного произнесения 3 с;

– число спектральных полос 8, (7 – для 8000Гц);

– центральные частоты по полосам 375, 500, 750, 1000, 1500, 2000, 3000, 4000 Гц, (400, 600, 800, 1200, 1600, 2400, 3200 – для 8000 Гц);

– вычисление отдельным параметром суммарной энергии сигнала по всем полосам на окне анализа;

– длина окна анализа 256 отсчетов;

– окна анализа не перекрываются;

– обнаружение границ речевого сигнала автоматическое по превышению порога паузы;

– определение порога паузы адаптивное;

– ввод произнесения через микрофон или из файла;

– параметризация речевого сигнала синхронно с его вводом,

– комбинированный алгоритм динамического программирования и градиентного спуска для временной нелинейной нормализации эталонного и тестового представлений речевых сигналов.

4.3.2. Интерфейс программы

После запуска программы, на экране появляется система голосового допуска, имеющая вид, представленный на рис. 4.4. В систему входят 4 пользователя и 5 помещений. Для удобства каждому пользователю присвоен цвет. На рис. 4.4 изображены следующие поля:

– присвоение имени пользователю;

– цвет пользователя, которому разрешен доступ;

– положение пользователя;

– протокол работы;

– выбор текущего пользователя;

– двери;

– кнопки управления положением текущего пользователя;

– назначение голосового пароля пользователю.

Рис. 4.4. Интерфейс программы Demo.exe.

4.3.3. Порядок работы с программой

4.3.3.1. Режим обучения. Сначала каждый пользователь должен записать свое имя в [1] (см. рис. 4.4), а затем нажать [8]. Система входит в режим запоминания голосового пароля. Система выдает сообщение: «Say your password», после которого необходимо произнести свой пароль. Система повторяет запрос от 2 до 4 раз, после чего выдает сообщение, либо «Bad recording quality» и обучение необходимо повторить снова, либо «Password is set» и обучение закончено. Пароли запоминаются в файле Demo.psw.

4.3.3.2. Режим распознавания. Сначала необходимо выбрать пользователя [5], под чьим именем вы желаете войти, и щелкнуть мышкой на соответствующей двери [6]. Система спросит пароль «Say your password» (от 1 до 3 раз). Если пароль будет успешно распознан, то система откроет дверь, в противном случае система откажет в доступе.

4.3.3.3. Общее. Для каждой комнаты заранее определено, кому разрешен доступ [2]. Выбор дверей производится с помощью [7]. Система отслеживает положение каждого пользователя [3] и ведет протокол работы [4].

В протоколе фиксируются все события, которые происходили при работе с системой:

- Time – время совершения события (текущее время);
- Id – номер пользователя (1-4, ? – если пользователь не узнан);
- Door – номер двери (1-6);
- Action – произошедшее событие:
    - Corridor => Room 4 – передвижение из коридора в комнату 4;
    - Alien – пользователь не зарегистрирован или не узнан;
    - Access denied – доступ в комнату запрещен;
    - Password of alien user – зарегистрированный пользователь пытался воспользоваться паролем другого зарегистрированного пользователя. Такую ситуацию можно смоделировать, если записать одного и того же пользователя с разными именами и паролями.

4.3.3.4. Замечание. Последнее сообщение показывает, что в данной программе реализовано решение открытой задачи идентификации по парольной фразе, поскольку на этапе Request происходит сравнение тестового произнесения со всеми эталонами, хранящимися в системе. После этого выбирается диктор с наиболее похожим эталоном, а потом принимается решение о принадлежности тестового произнесения выбранному диктору.

4.3.3.5. Проблемы. Если программа работает неверно, то проверьте следующее:

– правильность установки звуковой карты;

– возможность работы звуковой карты с 16-битными отсчетами;

– качество вводимого речевого сигнала.

Для исключения последнего необходимо оттестировать входной сигнал микрофона. Сделать это можно с помощью программы Audimic.exe, установив уровень записи примерно на 2/3 от максимума.

4.4. Контрольные вопросы

1. Как на сегодняшний день выглядит структура мирового рынка биометрических средств и систем?

2. Какая существует классификация биометрических средств защиты информации по биометрическим признакам, принципам действия и технологии реализации?

3. Какие подсистемы входят в число современных БСКД?

4. Чем характеризуются все биометрические системы?

5. Из каких пяти этапов состоит обобщенный алгоритм биометрической идентификации, характерный для всех известных БСЗИ?

6. Из каких основных блоков состоит схема типовой системы БСЗИ?

7. Что собой представляет технология распознавания голоса?

8. На чём основывается метод биометрической идентификации личности по радужной оболочке глаза?

9. На чём основывается метод биометрической идентификации личности по геометрии кисти руки?

10. Что собой представляет технология идентификация человека по геометрии лица?

11. Какие сочетания различных методов биометрической идентификации могут применяться для распознавания личности?

12. Какие приложения может использовать комбинированная (мультимодальная) биометрическая система для охвата различных типов биометрических данных?

13. Какие основные направления практического внедрения средств биометрического контроля доступа к информации существуют в настоящее время?

14. С какими новыми информационными технологиями взаимодействуют последние разработки БСЗИ?

4.5. Задание

1. Изучить описание и порядок работы с программой Demo.exe, приведённые в подразделе 4.3.

2. С помощью программы Demo.exe сымитировать все возможные вариант событий, которые могут произойти в процессе функционирования системы допуска в помещение с голосовым замком, описанные в подпункте 4.3.3.3.

3. Показать выполнение лабораторной работы преподавателю.

4.6. Содержание отчета

1. Цель работы.

2. Протокол событий, которые происходили при работе с системой допуска в помещение с голосовым замком.

3. Схема размещения оборудования разработанной биометрической системы безопасности на плане объекта, выданном преподавателем.

4. Конкретные предложения по снижению затрат на проектирование удобной архитектуры биометрической системы безопасности в соответствии с планом выбранного объекта.

5. Выводы по работе.

ЛИТЕРАТУРА

1. Абалмазов, Э. И. Методы и инженерно-технические средства противодействия информационным угрозам / Э. И. Абалмазов – М.: Изд-во «Компания «Гротек», 1997. – 246 с.
2. Андрианов, В. И. «Шпионские штучки» и устройства для защиты объектов и информации : справочное пособие / В. И. Андрианов [и др.] – СПб.: Лань, 1996. – 272 с.
3. Брюхомицкий, Ю. А. Учебно-методическое пособие к циклу лабораторных работ «Исследование биометрических систем динамической аутентификации пользователей ПК по рукописному и клавиатурному почеркам» по курсу: «Защита информационных процессов в компьютерных системах» / Ю. А. Брюхомицкий, М. Н. Казарин. – Таганрог: Изд-во ТРТУ, 2004. – 38 с.
4. Липов, В. Е. «Юнитроник» система охранно-пожарной сигнализации и управления : руководство по проектированию и типовые схемы подключения / В. Е. Липов, И. Г. Гооге. – М.: ЗАО «ЮНИТЕСТ», 2003. – 19 с.
5. Охранная видеотехника [Электронный ресурс] : справочник по телевизионным системам наблюдения для проектировщиков, консультантов и пользователей. – Электронные данные. – Режим доступа: http://secpro.narod.ru/13dowloads/ntdsecpro/21lit/videotech.pdf/.
6. Петраков, А. В. Основы практической защиты информации / А. В. Петраков. – М.: Радио и связь, 1999. – 368 с.
7. Петраков, А. В. Охрана и защита современного предприятия / А. В. Петраков, П. С. Дорошенко, Н. В. Савлуков. – М.: Энергоатомиздат, 1999. – 568 с.
8. Системы контроля доступа [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.videoglaz.ru/.
9. Торокин, А. А. Основы инженерно-технической защиты информации / А. А. Торокин. – М.: «Ось-89», 1998. – 334 с.
10. Уточкин, С. Основы работы с VideoCAD [Электронный ресурс] / С. Уточкин. – Электронные данные. – Режим доступа: http://cctvcad.com/rus/quick_start.htm/.
11. Хореев, А. А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации : учебное пособие / А. А. Хореев. – М.: Гостехкомиссия России, 1998. – 320 с.
12. ЮНИТЕСТ [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.unitest.ru/.

ПРИЛОЖЕНИЕ А

ПРИМЕРЫ СХЕМ РАЗМЕЩЕНИЯ ОБОРУДОВАНИЯ

Таблица А.1

Условные обозначения

Обозначение	Наименование
ARK	Прибор приемно-контрольный пожарный и управления.
ПР-2	Модуль управления пожарный ПР-2.
БРП	Блок резервного питания.
ВТН	Извещатель пожарный дымовой.
ВТМ	Извещатель пожарный ручной.
ВТК	Извещатель пожарный тепловой.
ARK 1	Пульт управления
BIAL/S	Оповещатель светозвуковой.
BIAS	Оповещатель звуковой.
BIAL	Оповещатель световой.
АМ	Метка адресная пожарная (МА-7ТК)
УШУ	Устройство шлейфовое управляющее УШУ-1.
КДУ	Клапан дымоудаления с электромеханическим приводом.
ZC	Резистор оконечный.
УОС	Устройство обрыва связи/датчик положения пожарного крана ДППК.

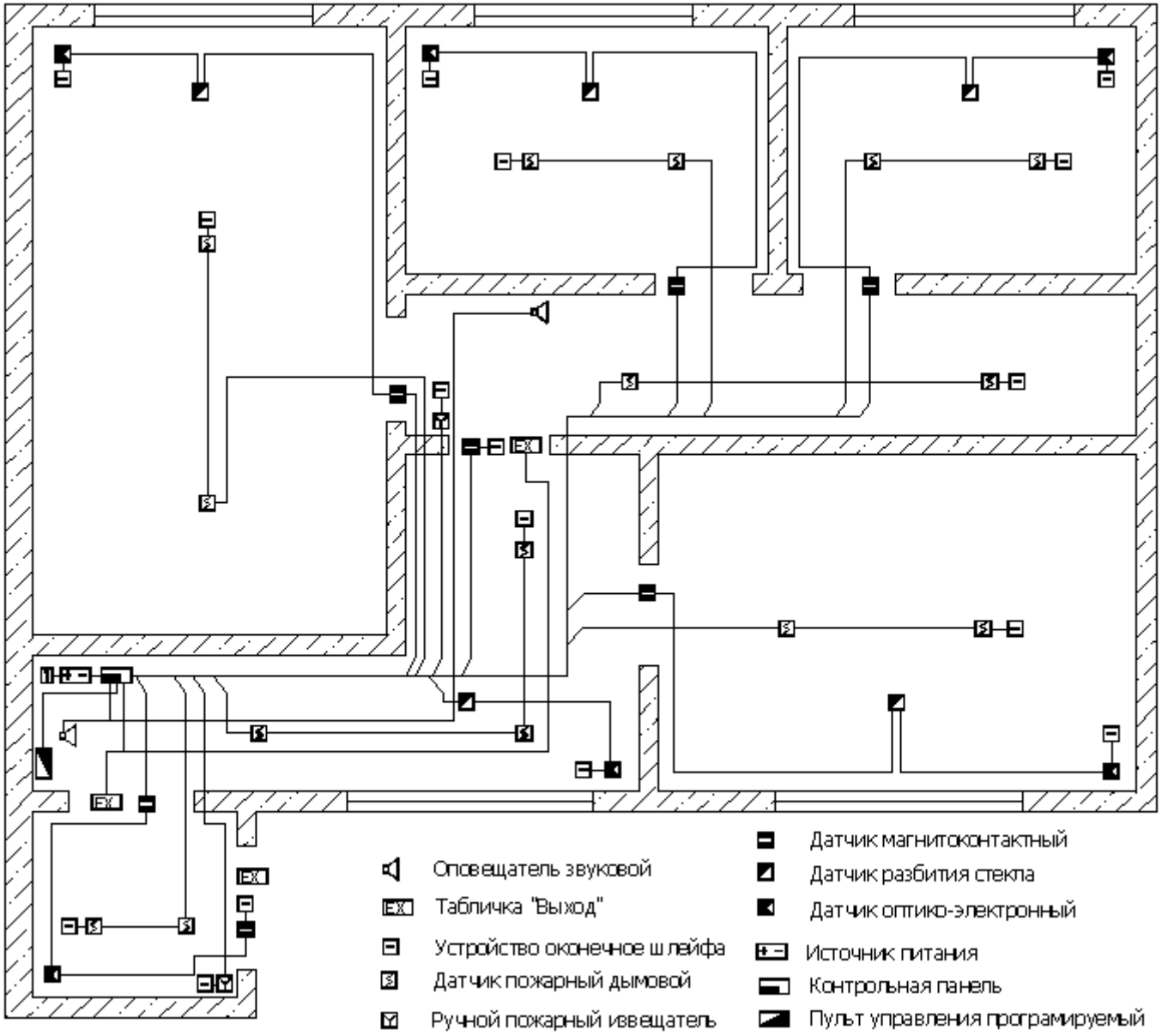

Рис. А.1. Схема размещения оборудования системы охранно-пожарной сигнализации.

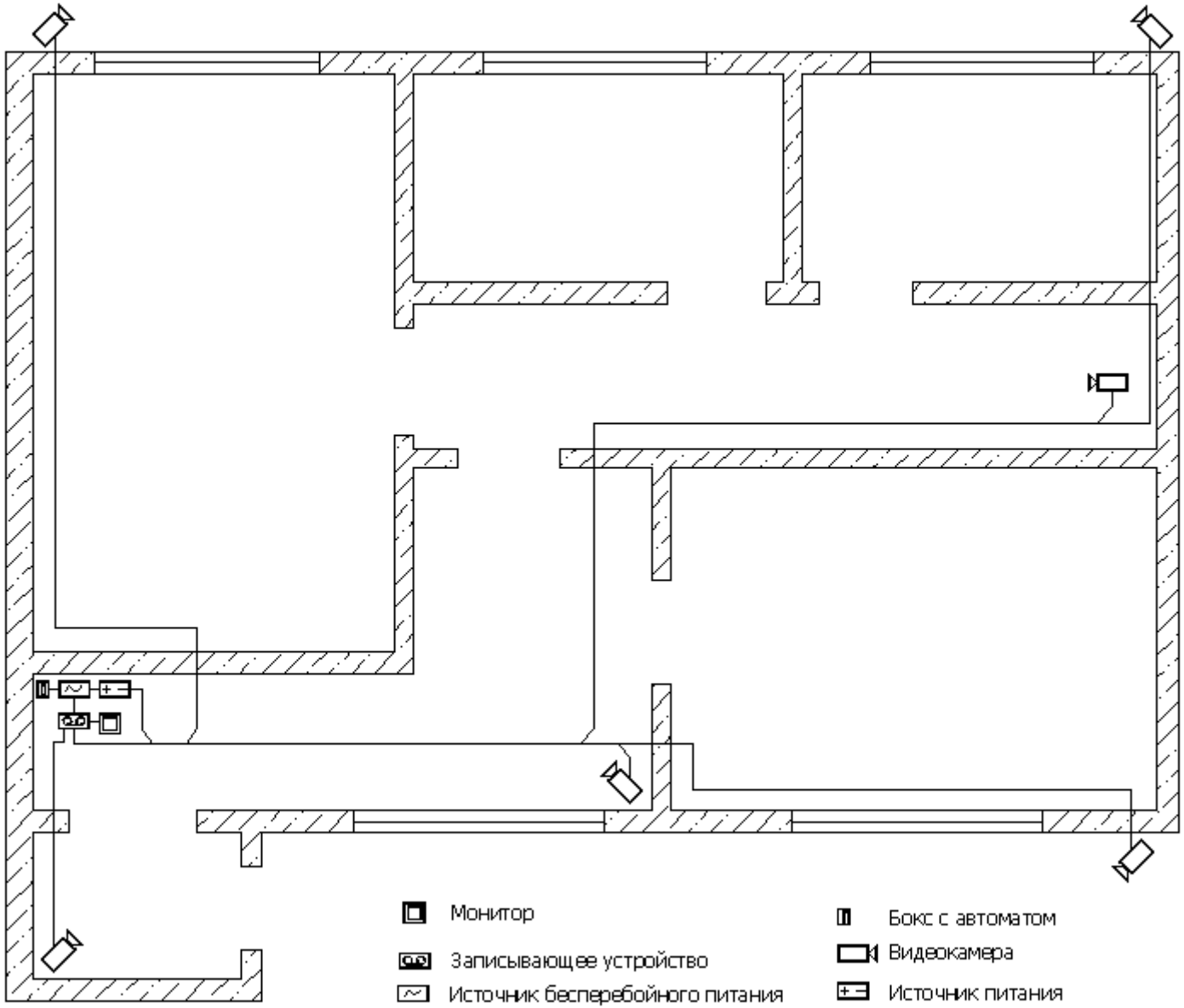

Рис. А.2. Схема размещения оборудования системы видеонаблюдения.

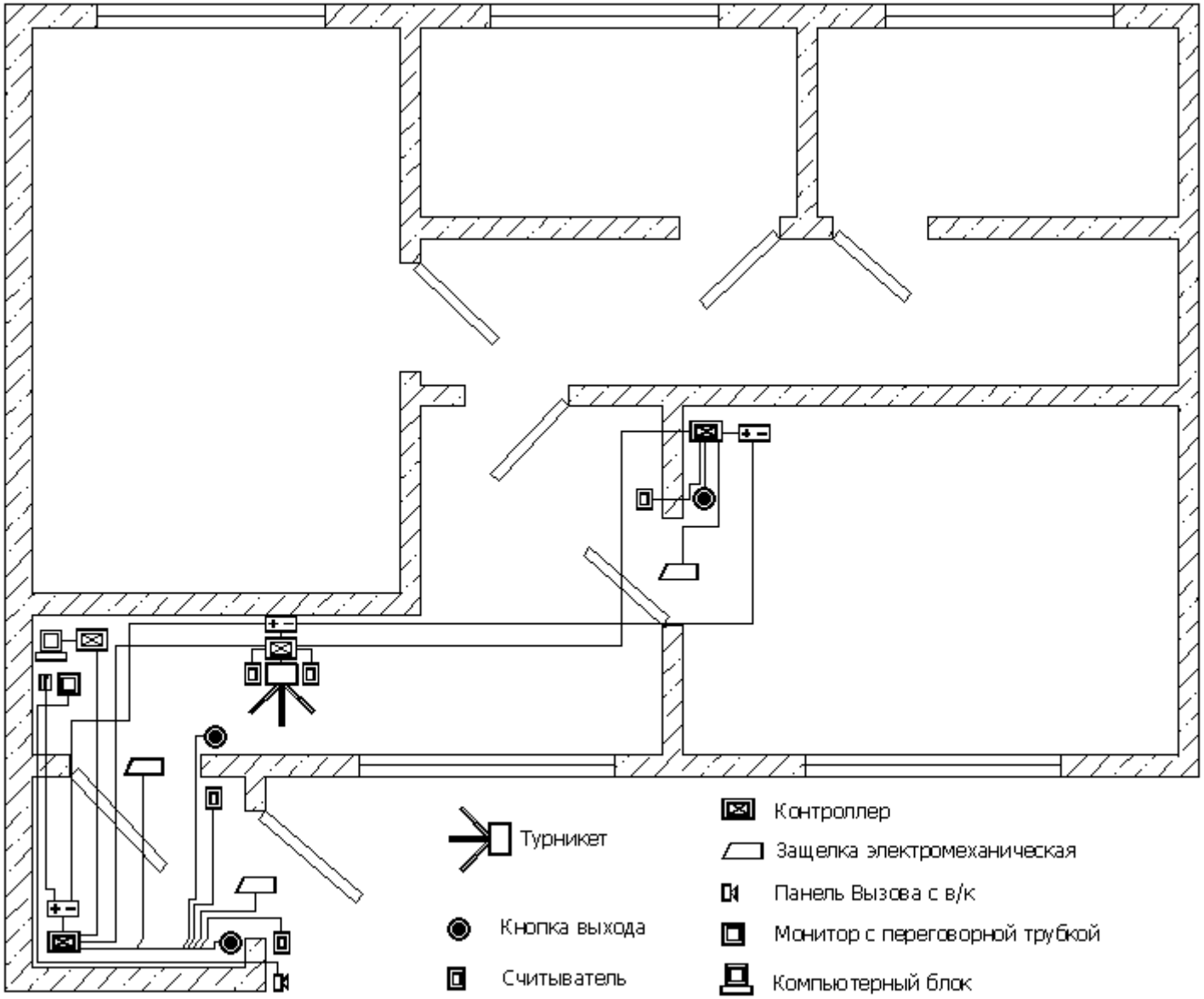

Рис. А.3. Схема размещения оборудования системы контроля доступа.

Св. план 2008, поз. 5

Учебное издание

Логин Владимир Михайлович
Будник Артур Владимирович

ТЕХНИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ

ЛАБОРАТОРНЫЙ ПРАКТИКУМ
по курсу **Физические и аппаратные средства защиты информации и их проектирование**
для студентов специальности
I-38 02 03 «Техническое обеспечение безопасности»
всех форм обучения

Редактор Н. В. Гриневич
Дизайн обложки У. Е. Шевчик

Подписано в печать 00.00.2007. Формат 60x84 1/16. Бумага офсетная.
Гарнитура «Таймс». Печать ризографическая. Усл. печ. л.
Уч.-изд. л. 4. Тираж 100 экз. Заказ 000.

Издатель и полиграфическое исполнение: Учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0056964 от 01.04.2004. ЛП №02330/0131666 от 30.04.2004.
220013, Минск, П. Бровки, 6