ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ
Государственное образовательное учреждение высшего профессионального образования
«ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Декан ФТФ
_____ В.И. Бойко
«10» декабря 2008 г.

Б.П. Степанов

ТЕХНИЧЕСКИЕ СРЕДСТВА СИСТЕМ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ ЯДЕРНОМУ ТЕРРОРИЗМУ

Методические указания к выполнению лабораторных работ
по курсу «Безопасность эксплуатации ядерных энергетических установок»
для магистрантов, обучающихся по специальности
«Физико-технические проблемы атомной энергетики»
направления 010700 «Физика»

Издательство
Томского политехнического университета
2008

УДК 621.039.577(076.5)
ББК 31.46я73
С79

Степанов Б.П.

С79 Технические средства систем безопасности и противодействия ядерному терроризму: методические указания к выполнению лабораторных работ по курсу «Безопасность эксплуатации ядерных энергетических установок» для магистрантов, обучающихся по специальности «Физико-технические проблемы атомной энергетики» направления 010700 «Физика» / Б.П. Степанов. – Томск: Изд-во Томского политехнического университета, 2008. – 40 с.

ISBN 5-98298-292-X

УДК 621.039.577(076.5)
ББК 31.46я7

Методические указания рассмотрены и рекомендованы
к изданию методическим семинаром кафедры
физико-энергетических установок ФТФ ТПУ
«29» ноября 2008 г.

Председатель
учебно-методической комиссии,
доктор физико-математических наук,
профессор,
заведующий кафедрой 21
физико-энергетических установок _____ *В.И. Бойко*

Рецензент

Кандидат технических наук, доцент ТПУ

В.Ф. Дядик

ISBN 5-98298-292-X

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В методических указаниях к лабораторным работам рассмотрены основные компоненты и технические средства систем безопасности и противодействия ядерному терроризму. Лабораторные работы предназначены для ознакомления с принципами функционирования радиационных мониторов, систем охраны периметра объекта, приобретения практических навыков работы с охранным оборудованием и средствами обнаружения, а также изучению методов построения и функционирования технических средств систем физической защиты (СФЗ) как по отдельности, так и в виде интегрированной системы. В лабораторный практикум входят пять следующих работ:

1. Изучение работы периметровых средств обнаружения.
2. Построение и моделирование системы контроля и управления доступом.
3. Изучение работы радиационного монитора, совмещенного с металлоискателем.
4. Моделирование работы системы контроля и управления доступом (СКУД), имеющей в своем составе биометрический считыватель.
5. Изучение работы системы видеонаблюдения.

Согласно правилам физической защиты ядерных материалов (ЯМ), ядерных установок и пунктов хранения ядерных материалов [1] система физической защиты (СФЗ) ядерного объекта (ЯО) включает в себя комплекс инженерно-технических средств, а также организационные мероприятия, направленные на их применение и совершенствование.

Основными задачами СФЗ являются:

1. Предупреждение несанкционированных действий.
2. Своевременное обнаружение несанкционированных действий.
3. Задержка (замедление) проникновения (продвижения) нарушителя.

При выполнении поставленных задач СФЗ ЯО должна выполнять функции обнаружения, задержки и ответного действия. Эти функции должны быть выполнены на протяжении периода времени, продолжительность которого меньше, чем продолжительность времени, требуемого для выполнения нарушителями своих целей.

Своевременное обнаружение совершения или попытки совершения диверсии, хищения ЯМ, несанкционированного доступа, проноса (провоза) запрещенных предметов, вывода из строя средств физической защиты (ФЗ) достигается путем:

- организации охраны периметров охраняемых зон, контрольно-пропускных пунктов (КПП) и отдельных объектов;

- применения систем охранной сигнализации, технические средства обнаружения (СО) которых расположены по периметру охраняемых зон, зданий, сооружений, помещений, а также могут располагаться внутри сооружений, помещений;
- применения систем оптико-электронного наблюдения за периметрами охраняемых зон, контрольно-пропускными пунктами, охраняемыми зданиями, сооружениями, помещениями и подступами к ним;
- досмотра персонала, командированных лиц, посетителей и их вещей, в том числе с применением средств обнаружения проноса ЯМ, взрывчатых веществ и предметов из металла;
- своевременного выявления умышленного вывода из строя (попыток вывода из строя) инженерно-технических средств ФЗ (ИТСФЗ);
- монтажа и эксплуатации ИТСФЗ в строгом соответствии с проектной и эксплуатационной документацией;
- контроля состояния и работоспособности ИТСФЗ.

Комплекс технических средств ФЗ в составе ИТСФЗ предназначен для технической поддержки действий по обеспечению физической защиты ЯОО и размещенных (эксплуатируемых) на нем ЯМ, ядерных установок и пунктов хранения ядерных материалов.

Техническими средствами системы физической защиты являются элементы и устройства, входящие в состав следующих основных функциональных систем [1]:

а) охранная сигнализация;
б) тревожно-вызывная сигнализация (ТВС);
в) контроль и управление доступом;
г) оптико-электронное наблюдение (ОЭН) и оценка ситуации;
д) оперативная связь и оповещение (в том числе средства проводной связи и радиосвязи);
е) защита информации (ЗИ);
ж) обеспечение электропитания, освещения.

Структурная схема комплекса ИТСФЗ представлена на рис. 1. При создании и функционировании ФЗ ЯО особая роль отводится построению и реализации элементов, устройств технических средств СФЗ, от правильной и эффективной работы которых во многом зависит своевременное обнаружение и установление факта несанкционированных действий, а также принятие правильных действий по их предотвращению и ликвидации силами охраны.

Поэтому в данном лабораторном практикуме рассматриваются практические вопросы работы средств обнаружения подсистемы охранной сигнализации, элементов системы контроля и управления доступа, устройств оптико-электронного наблюдения, контроля проноса (выноса) запрещенных материалов и предметов, а также методы и способы их настройки и управления в составе автоматизированной системы ФЗ.

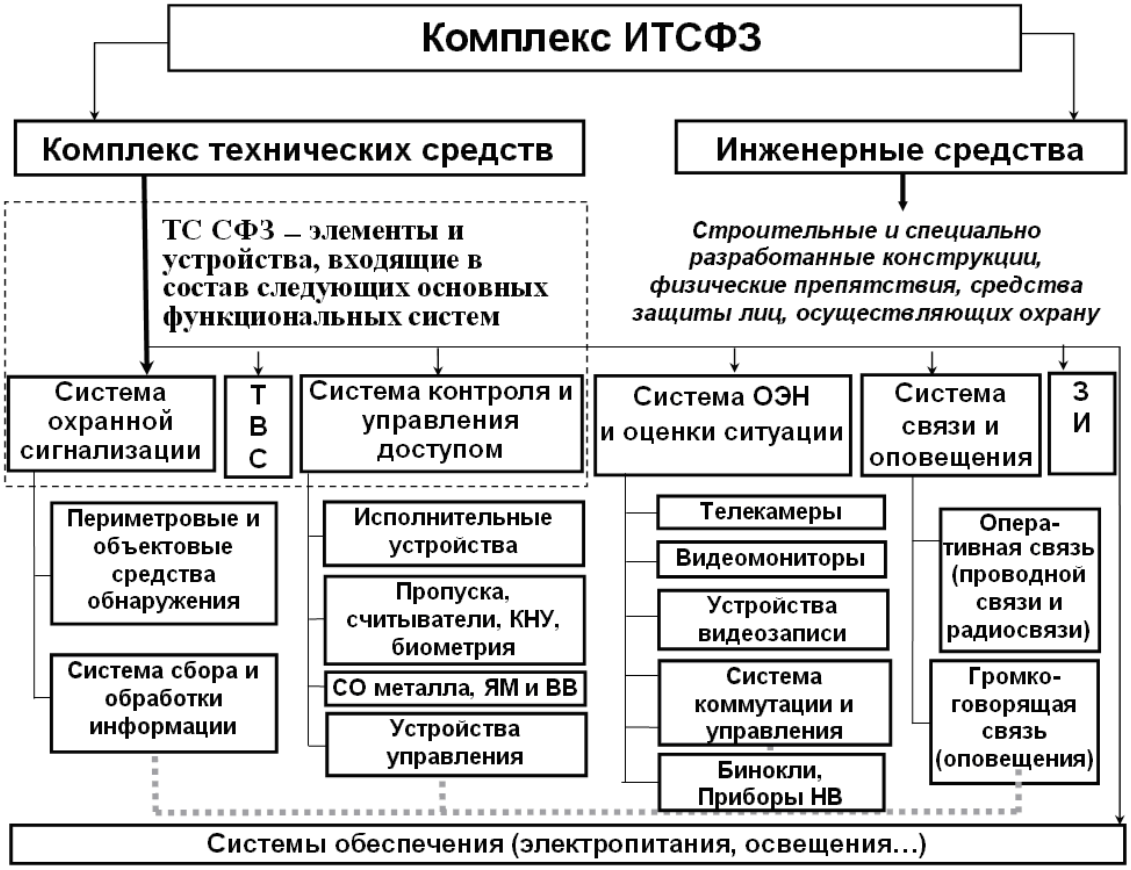

Рис. 1. Структурная схема комплекса ИТСФЗ

Лабораторная работа № 1
ИЗУЧЕНИЕ РАБОТЫ ПЕРИМЕТРОВЫХ СРЕДСТВ ОБНАРУЖЕНИЯ

Цель работы. Изучение вопросов организации периметра объекта и его оснащения устройствами охранной сигнализации, а также принципов действия, работы и настройки периметровых средств обнаружения.

ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Элементы подсистемы охранной сигнализации устанавливают факт несанкционированного действия, направленного на объект, и в рамках системы физической защиты выполняют функцию обнаружения проникновения на объект постороннего лица (нарушителя) или транспортного средства, пытающихся получить неразрешенный доступ на защищаемый участок.

Данная подсистема состоит из периметровых и объектовых средств обнаружения [1]. Периметровые средства обнаружения используются на открытой местности для блокирования участков периметра объекта, а объектовые средства обнаружения устанавливаются внутри зданий и помещений.

Защита периметра – один из наиболее важных элементов комплекса безопасности объекта, а системы охраны периметра являются электронными системами раннего обнаружения.

Специфика условий эксплуатации периметровых систем защиты заключается, прежде всего, в широком разнообразии климатических и почвенно-геологических условий. Большие сезонные колебания температуры, сильные снегопады, метели, мокрый снег, частые плотные туманы, ураганные ветры, сильные дожди, гололед, иней вызывают большие трудности при выборе соответствующих средств обнаружения и делают практически невозможным использование какой-либо единой системы для любой климатической зоны России. Также сами охраняемые периметры различаются по своим конструктивным, ландшафтным особенностям. Все это делает выбор конкретного устройства достаточно непростым делом и требует от проектировщика СФЗ хорошо ориентироваться в существующем многообразии выпускаемых средств обнаружения, знать их особенности, сферу наиболее эффективного применения и специфику использования.

Основными техническими характеристиками периметровых систем являются:

- вероятность обнаружения;
- наработка на ложное срабатывание;
- универсальность и гибкость средства обнаружения – возможность работы в широком диапазоне условий эксплуатации в различных климатических условиях для защиты разнообразных объектов;
- уязвимость системы, т. е. возможное преодоление рубежа без появления сигнала тревоги;
- маскировка (визуальная и техническая) средств обнаружения.

Для обнаружения факта вторжения человека в охраняемую зону используются самые различные физические принципы, позволяющие с той или иной вероятностью различить сигнал от находящегося в охраняемой зоне человека на фоне помеховых воздействий окружающей среды. В настоящее время при охране периметра применяются средства обнаружения, работающие на следующих физических принципах [2]: емкостные, радиолучевые, проводниковые (кабельные), оптико-лучевые, радиоволновые, магнитометрические, инфракрасные, вибрационные (деформационные), сейсмические, комбинированные.

ОПИСАНИЕ ЛАБОРАТОРНОГО СТЕНДА

В состав лабораторного стенда входят:

- извещатель охранный радиоволновый линейный «Радий-2»;
- датчик и модуль интерфейсный «Багульник-М»;
- прибор приемно-контрольный «КОДОС А-20»;
- адресный блок «КОДОС А-07/8»;
- адресный блок «КОДОС А-08»;
- сетевой контроллер «КОДОС СК-Е»;
- автоматизированное рабочее место.

Датчик регистрации преодоления заграждений «Багульник-М» с индексом 2КИ расшифровывается следующим образом:

2 – количество независимых охраняемых участков (каналов изделия);

К – основное назначение изделия, в данном случае, оборудование козырька или других инженерных сооружений из армированной скрученной колючей ленты (АСКЛ) или армированной колючей ленты (АКЛ);

И – наличие интерфейса RS-485.

Изделие в своей работе использует трибоэлектрический эффект, состоящий в возникновении ЭДС между проводниками в специально изготовленном кабеле (чувствительном элементе) при его деформации. Полученный от чувствительного элемента сигнал усиливается, селектируется и обрабатывается микропроцессором, где и принимается реше-

ние о выдаче сигналов тревоги или неисправности на станционную аппаратуру посредством размыкания соответствующих контрольных шлейфов или (и) по цифровому промышленному интерфейсу RS-485.

Изделие по функциональному назначению принадлежит к деформационным средствам охраны и предназначено для усиления охраны объектов различного назначения путём создания распределенного рубежа охраны и регистрации попыток его преодоления, с выдачей сигнала тревоги на станционную аппаратуру для принятия оперативных мер по их пресечению.

Основным назначением изделия является оборудование козырька из армированной скрученной колючей ленты (АСКЛ) или армированной колючей ленты (АКЛ) по верху основного ограждения или самостоятельных инженерных сооружений из АСКЛ (АКЛ).

Допускается использование изделия для защиты гибких сетчатых ограждений. В этом случае следует учитывать, что изделием будет фиксироваться только упругая деформация полотна ограждения с частотой 1÷2 Гц.

Данное изделие предназначено для применения совместно с приёмно-контрольными устройствами, фиксирующими изменение сопротивления или разрыв контрольной линии (шлейфа), и (или) с компьютеризированными приёмно-контрольными устройствами, поддерживающими цифровой промышленный интерфейс RS-485.

С помощью датчика «Багульник-М» обеспечивается создание охраняемого рубежа протяженностью до 410 метров**,** состоящего из двух независимых участков длиной до 205 метров каждый. При необходимости длина каждого из участков может быть увеличена до 410 метров без заметного ухудшения эксплуатационных характеристик изделия.

Изделие является двухканальным устройством. При обнаружении нарушения по какому-либо из участков формируется сигнал тревоги по соответствующему каналу. Устройство обеспечивает выдачу сигнала тревоги по двум каналам одновременно при открывании крышки блока обработки сигналов (БОС).

Подключение всех внешних цепей изделия к блоку обработки сигналов производится герметично при помощи разъёмов. Это позволяет при необходимости быстро заменить вышедшее из строя устройство и исключает возможность некачественного подключения чувствительных элементов.

Настройка изделия производится в цифровой форме с помощью клавиатуры и светодиодных индикаторов, расположенных на передней панели БОС. Два цифровых индикатора, шкальный индикатор уровня, а также два одиночных светодиодных индикатора позволяют получить полную информацию о состоянии устройства. Все параметры и на-

стройки изделия сохраняются при пропадании напряжения питания в энергонезависимой памяти устройства. Время хранения информации не менее 20 лет. При включении питания все параметры и настройки автоматически восстанавливаются. В энергонезависимой памяти также запоминается время наработки, отсчёт которого обеспечивает встроенный счётчик.

Питание изделия может осуществляться любым видом напряжения: постоянным, импульсным или переменным. Питающее напряжение может иметь пульсации произвольной формы и амплитуды, не превышающие по абсолютной величине максимальных напряжений питания устройства. Все внешние цепи изделия защищены от атмосферного и наведённого электричества, а также от кратковременных перегрузок. По всем внешним цепям реализована полная гальваническая развязка с напряжением пробоя изоляции от 500 до 2500 В (питание, интерфейс RS-485, выходные реле и входы ЧЭ). Устройство не выходит из строя при подключении питания обратной полярности, а также неправильной фазировке линий интерфейса RS-485.

Для получения оптимального соотношения сигнал/помеха в изделии применяется специально разработанный трибокабель, в котором величина возникающей ЭДС при деформации многократно повышена. Наличие в трибокабеле дополнительного внешнего экрана со 100%-м перекрытием (по которому не протекает ток контроля) позволяет практически полностью избавиться от электромагнитных и электростатических помех.

Конфигурация системы задается структурной схемой, которая приведена на рис. 1.1.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Ознакомиться со структурной схемой, назначением основных модулей и их техническими характеристиками, а также условиями эксплуатации предлагаемых периметровых устройств обнаружения.
2. Составить проект системы. Задать адресацию блоков согласно приведенным таблицам.
3. Проверить работоспособность и заданный алгоритм функционирования системы.

Проверка правильности выполненной коммутации проводится в виде тестовых испытаний в различных режимах, задаваемых преподавателем, и визуального наблюдения реакции системы на происходящие возмущения.

4. Ответить на контрольные вопросы.
5. Подготовить отчет.

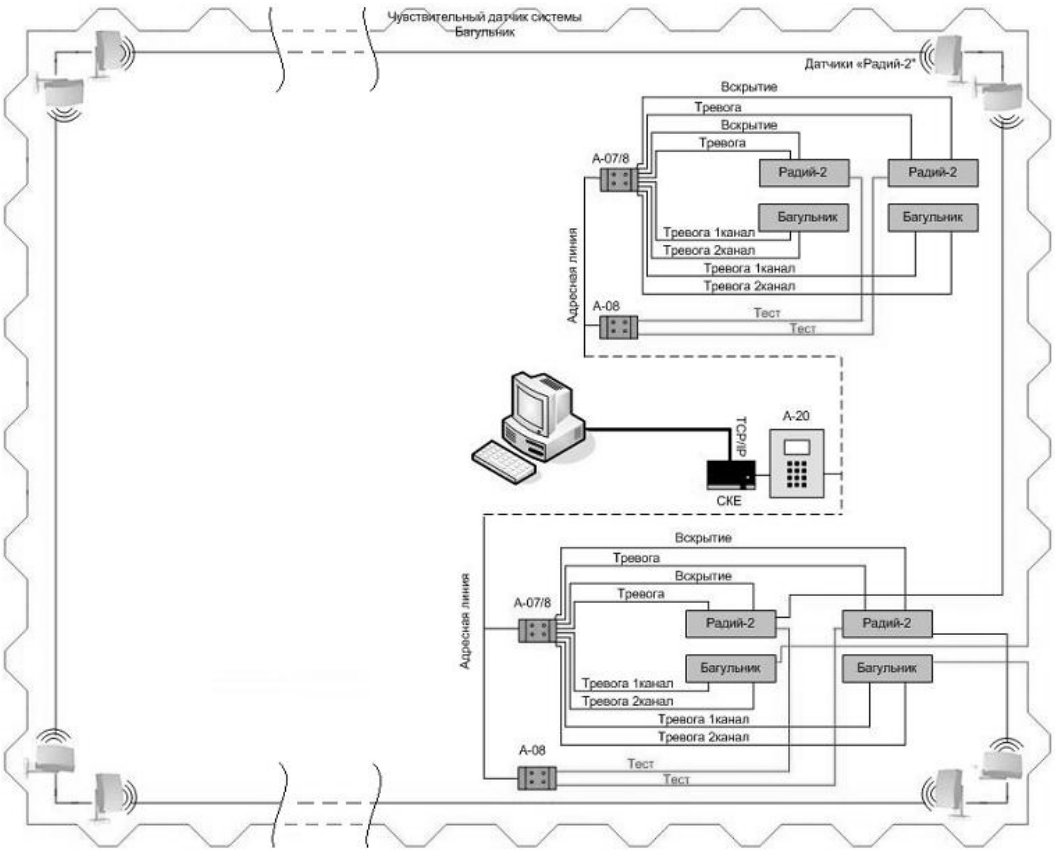

Рис. 1.1. Структурная схема периметровой защиты

Таблица 1

Порядок опроса адресных блоков

Порядковый номер опроса адресного блока	Аппаратный адрес блока	Тип блока
1		
2		
…		
N		

Таблица 2

Соответствие номеров зон и каналов порядковым номерам опроса и номерам клемм

Номер зоны или канала	Порядковый номер опроса адресного блока	Номер клеммы
1		
2		
…		
№ (не больше 200)		

Таблица 3

Состояние зон и каналов

Блок	Номер зоны / Параметр	1	2	…	N (не больше 200)
Х-1	Зона на охране				
	Контроль				
	Отложенное срабатывание				
	Автопостановка				
Х-2	Зона на охране				
	Инверсия				
	Контроль				
	Отложенное срабатывание				
	Отложенная постановка				
	Автопостановка				
Х-3	Канал активен				
	Контроль канала				
	Отложенное срабатывание				
	Время работы				
Х-4	Зона на охране				
	Инверсия				
	Контроль				

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Перечислите основные функции подсистемы охранной сигнализации.
2. Назовите специфические условия эксплуатации периметровых систем защиты.
3. На каких физических принципах работают средства обнаружения, устанавливаемые на периметре?
4. Опишите состав лабораторного стенда.
5. На каком физическом принципе работает средство обнаружения «Багульник-М»?
6. Основные характеристики устройства «Багульник-М».
7. Назовите и охарактеризуйте составные элементы структурной схемы периметровой защиты.

Список литературы

1. Правила физической защиты ядерных материалов (ЯМ), ядерных установок и пунктов хранения ядерных материалов.
2. Свирский Ю.К. Охранная сигнализация: средства обнаружения, коммуникации, управление // Системы безопасности. 1995. – № 4. – С. 10–16.
3. Датчик регистрации преодоления заграждении «Багульник-М(2КИ)»: руководство по эксплуатации. – М.: Изд-во ООО «Гос-Электро», 2002. – 27 с.

4. Система охранно-пожарной сигнализации на базе ППКОП «КОДОС А-20». Руководство по программированию и настройке. – М.: Изд-во НПК «СоюзСпецАвтоматика». – 48 с.
5. Система охранно-пожарной сигнализации на базе ППКОП «КОДОС А-20». Руководство по монтажу. – М.: Изд-во НПК «СоюзСпецАвтоматика». – 64 с.
6. Система охранно-пожарной сигнализации на базе ППКОП «КОДОС А-20». Руководство пользователя. – М.: Изд-во НПК «СоюзСпецАвтоматика». – 16 с.
7. Прибор приемно-контрольный охранно-пожарный «КОДОС А-20» – Базовый блок «КОДОС А-20». Руководство по эксплуатации. – М.: Изд-во НПК «СоюзСпецАвтоматика». – 8 с.
8. Прибор приемно-контрольный охранно-пожарный «КОДОС А-20» – Адоесный блок «КОДОС А-08». Руководство по эксплуатации. – М.: Изд-во НПК «СоюзСпецАвтоматика». – 8 с.

Лабораторная работа № 2
ПОСТРОЕНИЕ И МОДЕЛИРОВАНИЕ РАБОТЫ СИСТЕМЫ КОНТРОЛЯ И УПРАВЛЕНИЯ ДОСТУПОМ

Цель работы. Изучение принципов построения подсистемы контроля доступом и моделирование ее работы на примере управления турникетом и шлагбаумом.

ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Подсистема контроля и управления доступом (СКУД) в составе технических средств СФЗ представляет собой совокупность организационных мер, оборудования и приборов, инженерно-технических сооружений алгоритмов и программ, которая автоматически выполняет в определенных точках объекта и в заданные моменты времени, следующие основные задачи:

- разрешает проход уполномоченным субъектам (сотрудникам, посетителям, транспорту);
- запрещает проход всем остальным.

Система контроля и управления доступом (СКУД) предназначена для контроля и обеспечения санкционированного доступа персонала ЯО (посетителей, командированных лиц) и транспорта в (из) помещения, здания, сооружения, зоны и территории в соответствии с установленной на объекте режимно-правовой средой.

Согласно [1] СКУД должна обеспечивать:

- организацию доступа персонала ЯОО (командированных лиц и посетителей) и транспортных средств в соответствии с требованиями нормативных документов объектового уровня;
- исключение возможности несанкционированного доступа на территорию охраняемых зон за счет сговора с персоналом СФЗ, а также бесконтрольного прохода (проезда) через КПП;
- усиление требований по контролю права доступа лиц в охраняемые зоны в направлении от защищенной к особо важной зоне;
- протоколирование всех совершаемых действий, в том числе персоналом СФЗ и проходящими лицами, а также случаи силового воздействия на пропускные устройства;
- возможность изготовления пропусков как для постоянных сотрудников ЯОО и транспортных средств, так и посетителей и командировочных лиц, при этом должен вестись полный архив изготавливаемых и выдаваемых пропусков.

Поэтому организация СКУД на охраняемый объект является сложной и многоплановой задачей, решение которой требует детального изучения принципов организации самой системы доступа, а также алгоритмов функционирования исполнительных устройств (замков, турникетов и шлагбаумов).

При построении охраны ядерного объекта возникают задачи по организации санкционированного доступа на предприятие и в определенные помещения, а также по обеспечению возможности нахождения персонала на объекте в разрешенное время.

Обычно СКУД состоит из:

- набора карт-пропусков (ключей), которые выдаются пользователям системы;
- считывателей – устройств, идентифицирующих ключи;
- исполнительных устройств, которыми могут быть замки, шлагбаумы, турникеты и электроприводы ворот любых типов;
- контроллеров – интеллектуальных блоков, управляющих системой и принимающих решение о возможности прохода.

В качестве ключей-носителей признака могут использоваться карты различных типов: магнитные, Виганд, «проксимити» или же сам человек (как носитель индивидуальных биологических признаков), человеческая память, запоминающая набор цифр, которым является PIN-код (индивидуальный код пользователя) и др.

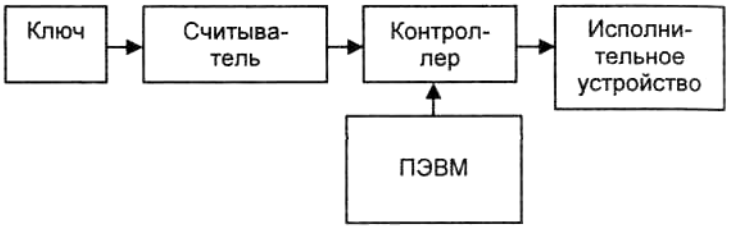

Рис. 2.1. Общая схема СКУД

Для съема информации с ключей предназначены устройства идентификации. В зависимости от типа носителя, естественно, меняются и устройства идентификации. Съем информации с различного вида карт осуществляют специальные считыватели, использующие те или иные физические принципы. Для съема информации о биологических признаках человека используют специальные биометрические считыватели (терминалы), а PIN-код вводится с клавиатур различных типов.

Информация, снимаемая с ключей, поступает в процессорный блок-контроллер, который ее обрабатывает, анализирует, принимает решение о возможности прохода. Любая система обязательно имеет плату, на которой размещаются микропроцессор и другие полупроводниковые элементы. Другой вопрос, где эта плата расположена: в отдельном блоке-контроллере, либо она вставлена прямо в корпус считывателя. У каждой из этих архитектур есть свои плюсы и минусы. Архитектура контроллера, совмещенного со считывателем, более устойчива к обрывам сети, но и менее защищена от взлома, так как блок, принимающий решения, расположен вне охраняемого помещения.

СКУД взаимодействует с персональным компьютером. В достаточно емких системах компьютер, используя специализированное программное обеспечение, полностью управляет контроллерами, собирает, обрабатывает и архивирует информацию, поступающую с объекта, осуществляет взаимодействие с сигнализацией и охранным телевидением.

Важнейшим элементом СКД является периферийное оборудование, поскольку именно оно вступает в непосредственный «физический контакт» с персоналом объекта в процессе идентификации и аутентификации личности и организации санкционированного доступа.

Идентификация – это процедура опознания объекта (человека-пользователя) по предъявленному идентификатору, установление тождества объекта или личности по совокупности общих и частных признаков. В отличие от идентификации, аутентификация подразумевает установление подлинности личности на основе сообщаемых проверяемым субъектом сведений о себе. Такие сведения называют идентификацион-

ными признаками. При проверке на КПП они представляют собой, как правило, персональные установочные данные (фамилия, имя, отчество), личный идентификационный номер (код), биометрические характеристики, однозначно определяющие личность пользователя перед системой. Идентификационные признаки или идентификаторы могут быть зафиксированы на материальном носителе (идентификационной карточке, пластиковом ключе), которые при проверке на КПП считываются аппаратурой или непосредственно в процессе проверки вводятся пользователем в систему через терминал. Для ввода идентификаторов пользователя в СКУД применяются следующие основные виды периферийного оборудования:

- кодонаборные терминалы;
- считывающие устройства;
- биометрические терминалы.

В архитектуре построения современных СКУД ядерных объектов можно выделить некоторые важные особенности. Так элементы СКУД применяются практически везде, где устанавливаются средства охранной сигнализации. Очень часто системы охранной сигнализации и СКУД взаимно дополняют друг друга при решении задач по охране находящихся в помещениях материальных и информационных ценностей. Современные СКУД позволяют контролировать состояние нескольких средств обнаружения (извещателей) и передавать сигналы о тревожных ситуациях на соответствующие пульты управления (ПУ). Примером может служить постановка (снятие) помещения под охрану (с охраны) при интеграции функций СКУД и системы охранной сигнализации. В простейшем случае первый из вошедших санкционированных пользователей снимает помещение с охраны, а последний из выходящих ставит его под охрану. Аналогично могут решаться вопросы интеграции с лифтами, инженерными системами объекта и т. п.

Идентификационные карточки, обладающие высокой степенью защищенности, изготавливаются специализированными фирмами на основе, как правило, закрытой технологии с использованием спецоборудования, не поставляемого на открытый рынок. Применяемая технология практически исключает возможность механического разделения элементов структуры идентификационной карточки без их значительного физического разрушения, легко определяемого контролером визуально. На основу карточки, запрессованной в прозрачную пластиковую пленку, наносятся как видимые идентификационные данные и фотография владельца, так и невидимая машиносчитываемая информация, благодаря которой обеспечивается повышенный уровень защищенности от попыток фальсификации и копирования.

Средства идентификации и аутентификации включают:

- идентификационные карточки;
- пластиковые ключи;
- терминалы.

Составными частями автоматизированной СКУД являются:

- сеть датчиков, обеспечивающих получение максимально полной информации со всего пространства, находящегося в поле зрения службы безопасности и позволяющая воссоздавать на центральном пульте наблюдения и управления всестороннюю объективную картину состояния помещений, всей территории объекта и работоспособности всей аппаратуры и оборудования, включенного в систему ФЗ;
- исполнительные устройства, способные при необходимости действовать автоматически или по команде оператора;
- пункты контроля и управления системой отображения информации, через которые операторы могут следить за работой всей системы в пределах своих полномочий;
- система сбора и обработки информации, наглядно представляющая информацию с датчиков и накапливающая ее для последующей обработки;
- коммуникации, по которым осуществляется обмен информацией между элементами системы и операторами.

При этом важно наличие возможности оперативного программирования (перепрограммирования) функций СКУД. Это позволяет противодействовать возможным несанкционированным действиям по выводу системы из строя.

ОПИСАНИЕ ЭКСПЕРИМЕНТАЛЬНОГО СТЕНДА

В состав лабораторного стенда входят:

- автоматизированное рабочее место (ПЭВМ);
- прибор приемно-контрольный «КОДОС ПРО»;
- контроллер «КОДОС ЕС-501»;
- контроллер «КОДОС ЕС-602»;
- считывающий турникетный контроллер «КОДОС RC-103»;
- турникет «PERCo-TTR-04.1»;
- шлагбаум «Game-G4000»;
- контроллер сетевой «КОДОС СКЕ-ЕС» ;
- считывающий контроллер «КОДОС RD-1100».

Конфигурация системы задается структурной схемой, представленной на рис. 2.2.

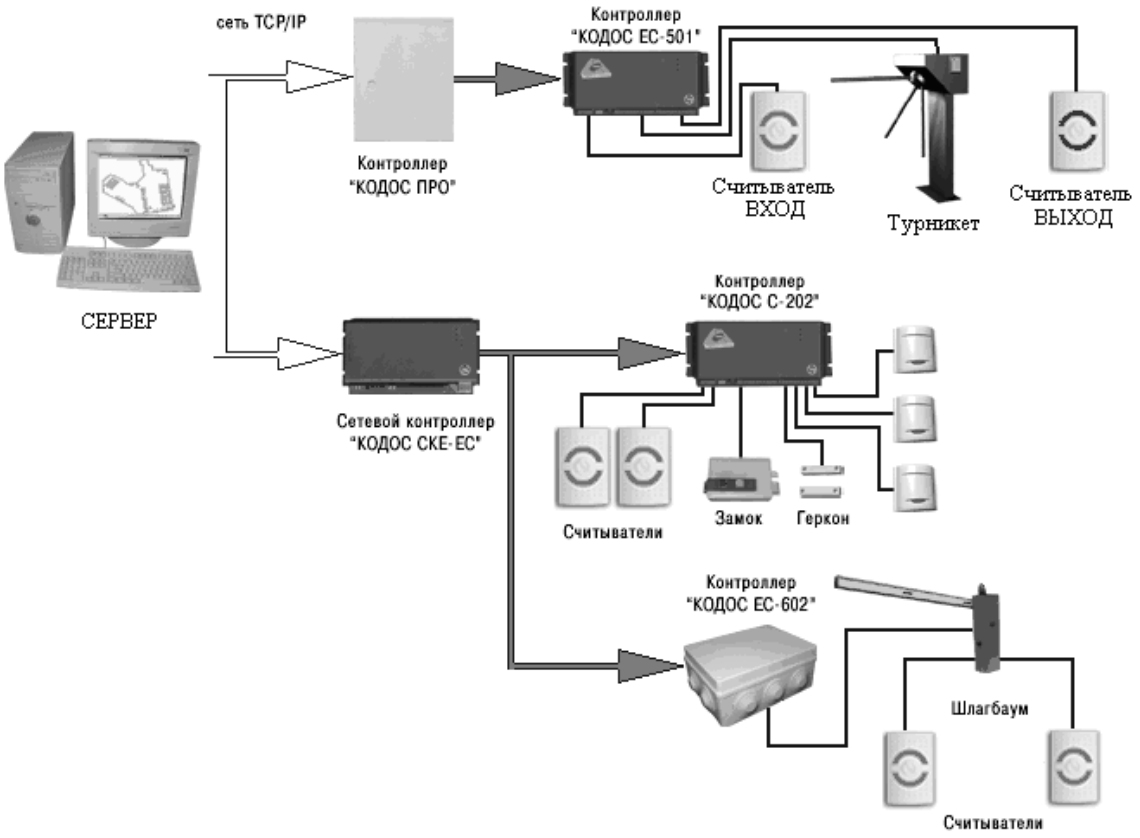

Рис. 2.2. Структурная схема моделируемой СКУД

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Изучить общие положения на электрическое подключение устройств.

2. Ознакомиться со структурной схемой СКУД, назначением входящих в нее модулей, техническими характеристиками и условиями эксплуатации исполнительных устройств.

3. Составить проект моделируемой СКУД.

4. Провести подключение исполнительных устройств: турникета и шлагбаума.

5. Организовать точки доступа, произвести регистрацию пользователей.

6. Заполнить таблицу состояний и полномочий.

7. Произвести подключение устройств СКУД.

Проверка правильности выполненных монтажных работ проводится в виде тестовых испытаний (в различных режимах) и визуального наблюдения реакции системы на происходящие события.

8. Ответить на контрольные вопросы и подготовить отчет.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Перечислите назначение СКУД и основные ее функции в системе физической защиты ядерного объекта.
2. Назовите состав СКУД, приведите ее общую схему и объясните взаимодействие отдельных элементов системы.
3. Раскройте смысл понятий: «идентификация» и «аутентификация».
4. Какие устройства служат для ввода идентификационных признаков?
5. Перечислите составные части автоматизированной СКУД.
6. Приведите структурную схему моделируемой СКУД.
7. Объясните назначение устройств, входящих в состав лабораторного стенда.

Список литературы

1. Правила физической защиты ядерных материалов (ЯМ), ядерных установок и пунктов хранения ядерных материалов.
2. Рольф М. Основы построения систем охранной сигнализации / пер. с англ. N Н-10736. – М.: ВЦП, 1984. – 71 с.
3. ГОСТ Р 51241–98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний
4. Контроллер «КОДОС ЕС-501». Руководство по эксплуатации. – М.: Изд-во НПК «СоюзСпецАвтоматика», 2008. – 26 с.
5. Оборудование для системы контроля и управления доступом «КОДОС» – Контроллеры «КОДОС ЕС-602», «КОДО ЕС-202». Руководство по эксплуатации. – М.: Изд-во НПК «СоюзСпецАвтоматика». – 28 с.
6. Оборудование для системы контроля и управления доступом «КОДОС» – Контроллер «КОДОС RC-103». Паспорт. – М.: Изд-во НПК «СоюзСпецАвтоматика», 2006. – 32 с.
7. Турникет электромеханический «PERCo-TTR-04.1». Руководство по эксплуатации. – Санкт-Петербург. – 32 с.
8. Считыватели «КОДОС RD-1100», «КОДОС RD-1040». Паспорт. – М.: Изд-во НПК «СоюзСпецАвтоматика», 2008. – 12 с.

Лабораторная работа № 3
ИЗУЧЕНИЕ РАБОТЫ СИСТЕМЫ РАДИАЦИОННОГО МОНИТОРИНГА

Цель работы. Изучение системы контроля и управления доступом, имеющую в своем составе радиационный монитор, совмещенный с металлодетектором.

ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

В состав СКУД на КПП должны входить средства, обеспечивающие досмотр проходящего персонала и проезжающего транспорта на предмет проноса (провоза) запрещенных предметов (оружия и других изделий из металла, ядерных и радиоактивных материалов, взрывчатых веществ и т. п.).

Радиационный монитор в составе СКУД предназначен для обнаружения на контрольно-пропускных пунктах делящихся ядерных материалов и радиоактивных веществ при их несанкционированном перемещении. Также правила физической защиты предписывают интегрировать такие мониторы с устройствами, обнаруживающими взрывчатые вещества и различные металлические предметы (запрещенные к проносу предметы).

Для решения указанных задач используют радиационные мониторы, которые делятся на два типа:

- стационарные (портальные), предназначенные для выявления объектов (пешеходов, транспорта, багажа, почтовых отправлений, бытовых и производственных материалов и отходов и т. п.) с повышенным (над естественным радиационным фоном) уровнем излучения;
- ручные, предназначенные для досмотра подозрительных объектов, выявленных стационарными радиационными мониторами, а также для обследования помещений и местности с целью определения мест радиационного загрязнения.

Пешеходные радиационные мониторы предназначены для обнаружения источников ионизирующего излучения и ядерных материалов по их гамма-излучению. Применяются на пешеходных контрольно-пропускных пунктах ядерных объектов.

ОПИСАНИЕ КОНСТРУКЦИИ РАДИАЦИОННОГО МОНИТОРА

Радиационный монитор представляет собой блок питания и управления (БПУ) с подсоединенными к нему блоками детектирования (БД), количество которых зависит от исполнения системы радиационного мониторинга (СРМ).

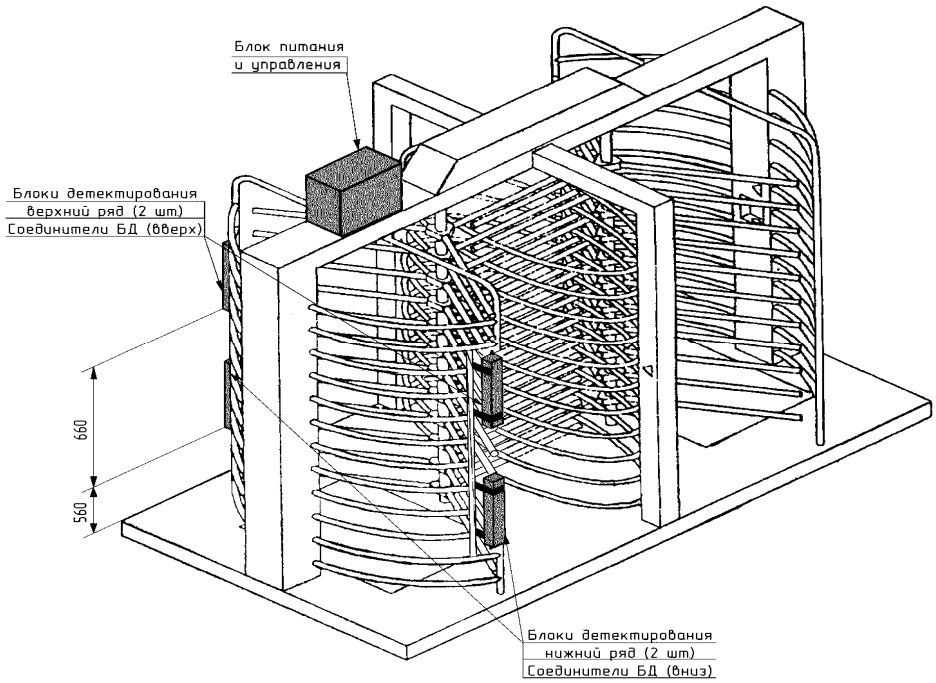

Рис. 3.1. Расположение блоков детектирования в турникете

Конструкция СРМ дает возможность подключения к БПУ до восьми БД, ПЭВМ, а также дополнительного оборудования (светофор, коробка распределительная, извещатель фотоэлектрический), что, наряду с возможностью широкого выбора длин соединительных жгутов, обеспечивает широкую область применения данного монитора.

Конструкционная гибкость СРМ позволяет эксплуатацию в составе различных шлюзовых кабин, турникетов, весовых платформ, конвейеров и пр., обеспечивая радиационный контроль пешеходов, транспорта и различных упаковок.

СРМ работает под управлением центрального процессора по программе, записанной в его постоянном запоминающем устройстве. Сигналы от БД поступают в БПУ, в котором центральный процессор в соответствии с алгоритмом считывает импульсы каждого БД, определяет средний фон для каждого БД и постоянно корректирует его значение с учетом его естественных колебаний. По результатам измерения счета фона процессор устанавливает порог тревоги.

При приходе команды о начале контроля объекта СРМ переходит в состояние контроля объекта, при этом центральный процессор определяет число импульсов от каждого БД за рабочий интервал и сравнивает это значение с указанным выше порогом тревоги. При превышении порога СРМ выдает сигнал ТРЕВОГА о наличии ДМ или РВ у объекта. Если счет ниже порога тревоги, монитор выдает короткий звуковой и световой сигналы о прохождении контроля.

Система радиационного мониторинга имеет следующие режимы работы:

I – самоконтроль (при включении напряжения питания);

II – первоначальное накопление фона;

III – работа.

В режиме I проверяются световые, звуковые и цифровые индикаторы, БД.

В режиме II измеряется первоначальное значение фона, вычисляется порог тревоги, проверяется соответствие счета фона заданным пределам.

В режиме III СРМ находится в одном из следующих состояний:

а) измерение фона;
б) контроль объекта;
в) остановка устройства.

Переход из одного состояния в другое производится по команде системы доступа (или оператора).

В состоянии «Измерение фона» СРМ непрерывно корректирует значение фона в соответствии с его колебаниями, проверяет его соответствие заданным пределам и корректирует порог тревоги.

«Контроль объекта» производится после прихода команды и может выполняться для двух режимов перемещения объекта контроля или их сочетания:

- режим ожидания, при котором СРМ однократно в течение заданного времени контроля измеряет излучение от объекта контроля, который остановлен в зоне контроля и ждет разрешения на выход;
- режим прохода, при котором СРМ многократно в течение рабочего интервала времени измеряет излучение от объекта контроля, пока он проходит зону контроля монитора с заданной скоростью в течение заданного времени контроля. Результаты контроля высвечиваются на цифровых индикаторах и могут передаваться на ЭВМ при необходимости.

По истечении времени контроля СРМ переходит в состояние «Останов.», в котором ожидает команду об окончании контроля, подтверждающую выход объекта из зоны контроля. В этом состоянии СРМ измерений (фона или объекта) не производит. По команде системы доступа СРМ переходит в состояние «Измерение фона». При непрерывном контроле объектов в режиме прохода СРМ проводит контроль, не ожидая команды управления.

Металлодетектор «НИКО-ВП-С» предназначен для осуществления индивидуального досмотра человека при проходе КПП ядерных объектов в целях обнаружения скрытых под одеждой человека и в его ручной клади металлических и металлосодержащих объектов, в том числе огнестрельного и холодного оружия, взрывных устройств на фоне других, менее металлоемких, не запрещенных к проносу предметов.

Принцип действия изделия основан на импульсном методе переходных процессов, возникающих в индуктивно-связанных контурах, образованных генераторными и приемными индуктивными рамками, расположенными в блоке обнаружения металлодетектора, а также контурами вихревых токов искомых металлических объектов, находящихся на теле (в одежде) человека и в его ручной клади.

ОПИСАНИЕ И РАБОТА СОСТАВНЫХ ЧАСТЕЙ ИЗДЕЛИЯ

1. Блок питания и управления

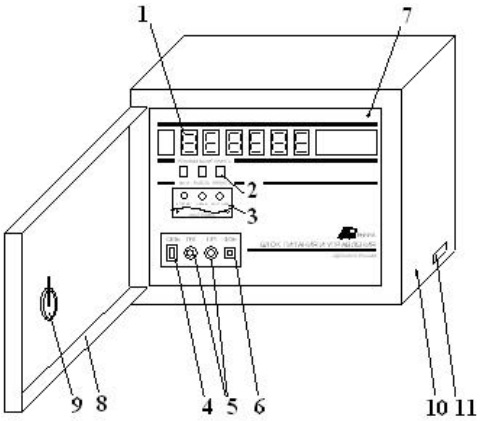

Рис. 3.2. Блок питания и управления

1 – цифровое табло;
2 – световые индикаторы состояния СРМ;
3 – клавиатура (кнопки);
4 – выключатель СЕТЬ;
5 – вставки плавкие;
6 – кнопка ФОН;
7 – пломба;
8 – дверца;
9 – замок;
10 – клемма заземления;
11 – маркировка

БПУ предназначен для питания БД, обработки сигналов БД, выдачи информации о наличии/отсутствии источников излучения в контролируемом объекте и связи с внешними устройствами.

В состав БПУ входит плата управления и блок питания, который вырабатывает напряжение +12 В и –12 В – для питания БД и +5 В – для питания платы управления БПУ.

Центральный процессор (ЦП) управляет работой СРМ по программе, записанной в его постоянном запоминающем устройстве. Для расширения и использования возможностей центрального процессора в плате управления установлено оперативное запоминающее устройств и электрически перепрограммируемое запоминающее устройство, в котором хранятся программные константы. Перепрограммирование констант производится автономно при помощи клавиатуры, расположенной на лицевой панели.

Блок реле обеспечивает связь СРМ с внешним управляющим устройством через соединитель УПР, которое управляет работой СРМ и снимает данные о состоянии (сигнализации), где находится СРМ.

Интерфейс связи обеспечивает связь СРМ с внешней ЭВМ по интерфейсу RS-232 или RS-485.

Индикация (ИНД) обеспечивает вывод данных о состоянии СРМ и результатах контроля в цифровой, визуальной и звуковой формах.

Ограничитель-формирователь предназначен для формирования по амплитуде и длительности импульсов, поступающих из блоков детектирования.

Блок счета импульсов (БСИ) предназначен для оперативного запоминания количество импульсов, поступающих от каждого БД за интервал времени 0,2 с, и передачи данных в ЦП.

Блок детектирования

БД предназначен для преобразования потока гамма-излучения в заданной области энергий в поток электрических импульсов стандартной формы и амплитуды напряжения.

БД соединяют с БПУ жгутами из комплекта поставки СРМ. При расположении БД под открытым небом они накрываются кожухами из комплекта СРМ для защиты от воздействия прямых осадков и солнечного света.

БД предназначен для преобразования потока гамма-излучения в заданной области энергий гамма-излучения ДМ в поток электрических импульсов стандартной формы и амплитуды напряжения.

В каждом БД имеется детектор гамма-излучения, состоящий из сцинтилляционного детектора и фотоэлектронного умножителя. Ионизирующее излучение от ДМ или РВ преобразуется сцинтиллятором в световые импульсы, которые преобразуются в электрические импульсы и усиливаются фотоэлектронным умножителем.

В усилителе-формирователе производится усиление и выделение импульсов фотоэлектронного умножителя по амплитуде, соответствующих излучению ДМ на основе урана-235 (в области от 50 до 305 кэВ), формирование их по длительности и амплитуде для передачи в БПУ, а также происходит формирование импульса светодиода, освещающего фотоэлектронный умножитель при самоконтроле БД. Преобразователь напряжения (ПН) предназначен для преобразования низковольтного напряжения питания в высокое напряжение для питания фотоэлектронного умножителя.

Коробка распределительная служит для коммутации светофоров и фотоэлектрического извещателя с БПУ при автоматическом контроле объектов.

Два светофора (входной и выходной) служат для сигнализации объекту контроля о начале контроля (входа в зону контроля) и об окон-

чании контроля (выходе из зоны контроля по окончании контроля) и обеспечивают автоматизацию процесса контроля. Светофоры подключаются к коробке распределительной и управляются БПУ.

Фотоэлектрический извещатель (изделие внешней поставки) состоит из передатчика и приемника, служит для регистрации нахождения объекта контроля в зоне контроля СРМ и обеспечивает автоматический запуск БПУ в состояние «Контроль объекта» из состояния «Измерение фона» при въезде объекта и в состояние «Фон» при выезде объекта.

Фотоэлектрический извещатель подключается к БПУ через коробку распределительную из зоны контроля.

В состав лабораторного стенда входят:

- радиационный монитор, совмещенный с металлодетектором;
- автоматизированное рабочее место;
- контроллер сетевой «КОДОС СКЕ-ЕС» ;
- прибор приемно-контрольный «КОДОС ПРО»;
- контроллер «КОДОС ЕС-602»;
- считывающий контроллер «КОДОС RD-1100».

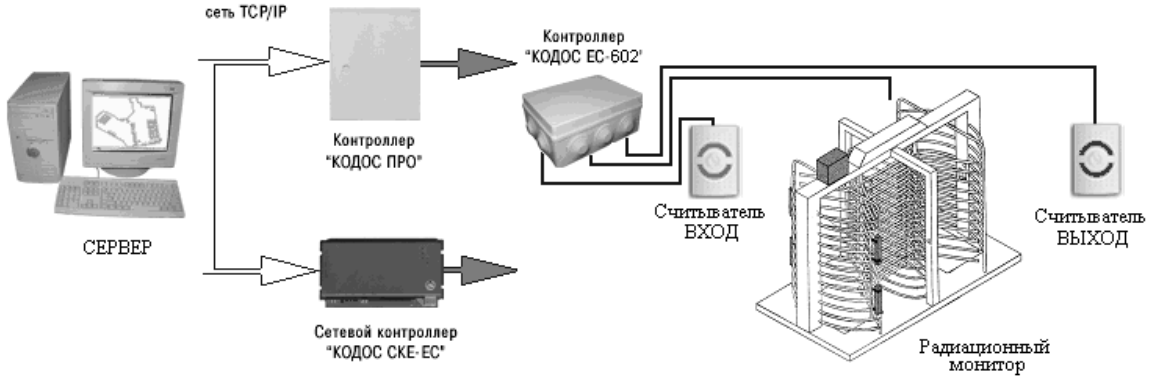

Рис. 3.3. Структурная схема системы радиационного мониторинга

Конфигурация системы задается следующей структурной схемой, представленной на рис. 3.3.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Внимательно изучить общие положения по подключению устройств.

2. Ознакомиться с назначением модулей и структурной схемой системы радиационного мониторинга, техническими характеристиками и условиями эксплуатации устройств.

3. Составить проект системы, который будет использоваться в следующих этапах (монтаж, подключение, пуск системы), в виде технической схемы с указанием мест размещения, зон покрытия и номеров каналов.

4. По согласованию с преподавателем приступить к монтажу и подключению устройств.

Прежде чем приступить к эксплуатации системы, необходимо тщательно изучить и произвести все необходимые настройки в точном соответствии с прилагаемыми описаниями и документацией.

5. Выполнить проверку работоспособности системы.

Проверка правильности выполненных монтажных работ проводится в виде тестовых испытаний (в различных режимах) и визуального наблюдения реакции системы на происходящие события.

Основной причиной неработоспособности системы является несоблюдение полярности при подключении устройств. Перечень возможных неисправностей и способов их устранения приведены в документации на соответствующие устройства.

6. Ответить на контрольные вопросы.

7. Подготовить отчет.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Чем определяется необходимость размещения на КПП систем радиационного мониторинга?
2. Какие типы радиационных мониторов применяются на КПП ядерных объектов?
3. Перечислите основные элементы радиационного монитора и режимы его работы.
4. Назначение встраиваемого в радиационный монитор металлодетектора.
5. Раскройте принципы действия блоков детектирования.
6. Для каких целей служат фотоэлектрический извещатель и светофоры, каким устройством они управляются и коммутируются?
7. Назовите основные элементы и устройства моделируемой системы радиационного мониторинга.

Список литературы

1. Демин Ю.И., Петраков А.В. Современные автоматизированные охранные системы: тезисы докладов на НТК МТУСИ. – 1993. – С. 9–10.
2. ГОСТ Р 51241–98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний
3. Оборудование для системы контроля и управления доступом «КОДОС» – Контроллеры «КОДОС ЕС-602», «КОДОС ЕС-202». Руководство по эксплуатации. – М.: Изд-во НПК «СоюзСпецАвтоматика», 2008. – 28 с.
4. Считыватели «КОДОС RD-1100», «КОДОС RD-1040». Паспорт. – М.: Изд-во НПК «СоюзСпецАвтоматика», 2008. – 12 с.

Лабораторная работа № 4
МОДЕЛИРОВАНИЕ РАБОТЫ СКУД, ИМЕЮЩЕЙ В СВОЕМ СОСТАВЕ БИОМЕТРИЧЕСКИЙ СЧИТЫВАТЕЛЬ

Цель работы. Построение и моделирование системы контроля управления доступом, в состав которой входит биометрический контроллер.

ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Биометрическая аутентификация является одной из компонент системы контроля и управления доступом (СКУД). В свою очередь СКУД необходима для разграничения прав доступа на объект или на его отдельные зоны.

Аутентификация – «проверка подлинности», тот ли это субъект за которого он себя выдаёт. Биометрия – это научная дисциплина, изучающая способы измерения различных параметров человека с целью установления сходства (различий) между людьми и выделения одного конкретного человека из множества других людей. Таким образом, биометрическая аутентификация – это процесс доказательства и проверки подлинности заявленного пользователем права доступа, через предъявление пользователем своего биометрического образа и путем преобразования этого образа в соответствии с заранее определенным протоколом аутентификации. Введём также понятие идентификации. Идентификация – это отождествление данного объекта с одним из известных системе объектов.

В последнее время наибольшее распространение получили методы аутентификации на основе следующих биометрических параметров: форма кисти руки, отпечаток пальца, рисунок радужной оболочки глаза.

В общем виде работа с биометрическими данными организована следующим образом. Сначала создается и поддерживается база данных характеристик потенциальных пользователей. Для этого биометрические характеристики пользователя снимаются, обрабатываются и результат обработки (называемый биометрическим шаблоном) заносится в базу данных. Хранятся данные в кодовом виде.

В дальнейшем для идентификации (и одновременно аутентификации) пользователя выполняются следующие этапы:

1) выделение зоны аутентификации;

2) сканирование изображения (папиллярный узор, сетчатка, рисунок вен и т. д.), запись звука с последующим вводом;

3) кодирование этого изображения или звука;

4) сравнение полученного кода с тем кодом, который есть в базе данных;

5) принятие решения об управлении доступом.

Распознавание отпечатка пальца основано на анализе распределения особых точек (концевых точек и точек разветвления папиллярных линий), которые характеризуются их местоположением в декартовых координатах. Для снятия отпечатков в режиме реального времени применяются специальные контактные датчики различных типов.

ПРИНЦИП РАБОТЫ СКУД НА ОСНОВЕ BIOSMART-КОНТРОЛЛЕРОВ

Отличительной особенностью BioSmart-контроллеров является использование емкостных сканеров отпечатков пальцев, вместо традиционных оптических. Вследствие этого данное устройство обладает более высокими техническими характеристиками:

- качественный цифровой образ отпечатков пальца;
- минимальное время сканирования, порядка 1секунды;
- аппаратная защита от муляжей;
- сверхтонкий размер, толщина сканера – 3 миллиметра.

Регистрация пользователей производится с помощью ПО BioSmart-Studio и контрольного считывателя, подключаемого через USB порт персонального компьютера. На каждого пользователя можно зарегистрировать до 10 отпечатков пальцев (обычно 2–4). Далее пользователю присваиваются права доступа на конкретные точки прохода, при этом информация об отпечатках пальцев пользователя в кодированном виде передается по линии связи в контроллер.

Когда пользователь прикладывает палец к сканеру контроллера BioSmart, происходит поиск в базе данных контроллера зарегистрированных отпечатков. При успешной идентификации контроллер выдает управляющий сигнал на блок управления реле, который в свою очередь включает исполнительные устройства (электромагнитные замки, турникеты и пр.), в журнал событий записывается соответствующая информация. В случае неуспешной идентификации фиксируется событие об отказе доступа. Среднее время сканирования и распознавания отпечатков пользователя составляет не более одной секунды.

Контроллер BioSmart может работать с внешними датчиками. На блоке управления реле предусмотрены два дискретных входа. Первый дискретный вход применяется для подключения выносной кнопки для выхода из помещения. При этом событие нажатия кнопки также фиксируется в журнале. Второй дискретный вход может применяться для подключения датчика к пожарной сигнализации. В случае пожара и срабатывания датчика дверь беспрепятственно откроется.

В качестве внешнего коммуникационного интерфейса связи контроллера BioSmart применяется RS-485, подключение по витой паре, максимальная удаленность от сервера составляет до 500 метров. Для

защиты от внешних перенапряжений используется гальваническая развязка 3 кВ. Линия связи должна подключаться к серверу через специальный преобразователь USB – RS-485 или Ethernet – RS-485.

Контроллер BioSmart имеет возможность интеграции с уже существующей системой контроля доступа на предприятии. Для этого предусмотрены вход и выход интерфейса Wiegand. К входному интерфейсу Wiegand можно подключить стандартный считыватель магнитных карт. При этом будет возможна организация пропускного режима по карте или по отпечатку, а также совместный режим работы, сначала необходимо приложить карточку к проксимити-считывателю, потом палец к биометрическому считывателю. Выход Wiegand контроллера BioSmart можно подключить к входу контроллера системы контроля доступа стороннего производителя. Таким образом можно существенно повысить безопасность на предприятии, где уже установлена система контроля доступа по пластиковым картам.

Контроллер биометрический BioSmart – электронный модуль предназначенный для идентификации отпечатков пальцев. Контроллер способен хранить в своей энергонезависимой памяти до 9000 отпечатков пальцев и 12800 событий. Все события в контроллере записываются в хронологическом порядке с указанием точного времени.

Контрольный считыватель Futronic FS 80 предназначен для регистрации пользователей в СКУД с BioSmart.

Конфигурация системы задается структурной схемой, приведенной на рис. 4.1.

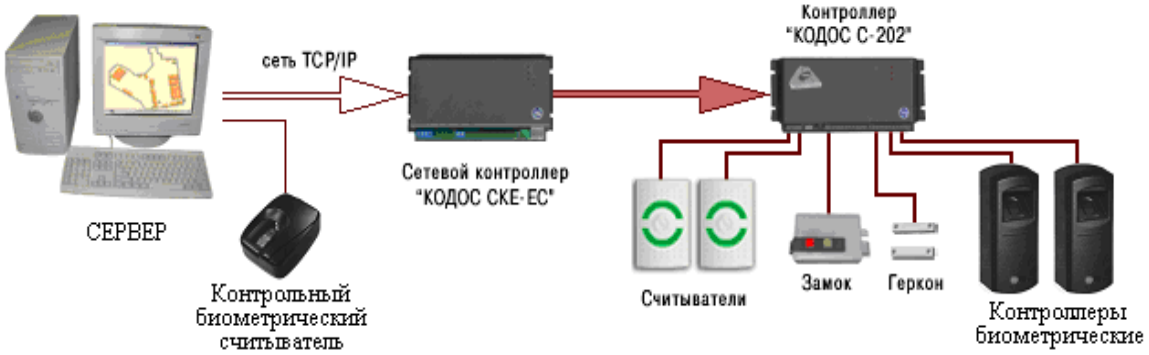

Рис. 4.1. Структурная схема СКУД
на основе биометрического считывателя

В состав лабораторного стенда входят:

- автоматизированное рабочее место;
- контроллер сетевой «КОДОС СКЕ-ЕС» ;
- считывающий дверной контроллер «КОДОС RC-102»;
- считывающий биометрический контроллер «BioSmart»;

- контрольный считыватель «Fultronic FS 80 «;
- электромагнитный (или электромеханический) замок;
- индикатор положения двери (геркон).

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Внимательно изучить общие положения, инструкции по эксплуатации устройств и модулей.
2. Ознакомиться с назначением модулей создаваемой СКУД.
3. Изучить технические характеристики и условия эксплуатации устройств.
4. Составить проект моделируемой системы.
5. Выполнить монтаж и подключение устройств между собой.

Прежде чем приступить к эксплуатации системы, необходимо тщательно изучить и произвести все необходимые настройки в точном соответствии с прилагаемыми описаниями и документацией.

6. Провести проверку работоспособности системы.

Проверка правильности выполненных монтажных работ проводится в виде тестовых испытаний (в различных режимах) и визуального наблюдения реакции системы на происходящие события.

7. Ответить на контрольные вопросы.
8. Подготовить отчет.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Принципы идентификации аутентификации в системах контроля и управления доступом.
2. Перечислите методы аутентификации с применением биометрических параметров.
3. Назовите основные этапы биометрической аутентификации.
4. Раскройте принципы работы BioSmart-контроллера.
5. Как происходит регистрация пользователей в СКУД на основе биометрического считывателя.
6. Перечислите компоненты моделируемой СКУД, раскройте их назначение.

Список литературы

1. ГОСТ Р 51241–98. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.
2. Оборудование для системы контроля и управления доступом «КОДОС» – Контроллер «КОДОС RC-102». Паспорт. – М.: Изд-во НПК «СоюзСпецАвтоматика», 2008. – 32 с.

Лабораторная работа № 5
ПОСТРОЕНИЕ СИСТЕМЫ ВИДЕОНАБЛЮДЕНИЯ

Цель работы. Изучение вопросов построения и принципов функционирования системы охранного видеонаблюдения, как составляющей технических средств системы физической защиты ядерного объекта, и создание автоматизированного рабочего места на основе программного обеспечения «КОДОС-ВИДЕОСЕТЬ».

ОСНОВНЫЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Системы видеонаблюдения играют наиболее существенную роль в структуре системы ФЗ, так как выводят систему охраны объекта на качественно более высокий уровень. Любое средство охранной сигнализации в ответ на внешнее воздействие, характерное для нарушителя, находящегося в охраняемой зоне, вырабатывает сигнал тревоги с определенной вероятностью обнаружения. Существует и возможность ложной подачи тревоги. Это вызывает необходимость наличия средства идентификации оператором процессов, происходящих в охраняемых зонах и на подступах к ним. В качестве таких средств наиболее оптимально с позиций восприятия человеком-оператором применение системы оптико-электронного наблюдения[1].

Ценность системы видеонаблюдения состоит в том, что она позволяет получить визуальную картину состояния охраняемого объекта, обладающую такой высокой информативностью, какую не могут дать никакие другие технические средства охраны. При этом оператор находится вдали от зоны наблюдения (т. е. на безопасном расстоянии). Это создает ему условия и дополнительное время для анализа ситуации и принятия решения об организации ответных действий.

Рассмотрим основные компоненты системы телевизионного наблюдения.

Телевизионная камера – это устройство, которое преобразует оптическое изображение наблюдаемого объекта (сцены) в электрический видеосигнал определенного стандарта (набора требований к структуре и характеру составляющих видеосигнала, позволяющего стандартизировать процесс приема/передачи видеоизображений). Телекамера является важнейшим элементом системы, так как именно с нее в систему поступает первичная информация об объекте и именно ее характеристиками определяется качество изображения в целом. Камера представляет собой электронную плату, на которой размещен чувствительный элемент – матрица, выполненная на приборах с зарядовой связью (ПЗС-

матрица), и объектив. Более простые (и, соответственно, более дешевые) камеры оснащаются, как правило, простейшими встроенными объективами, более дорогие – сменными объективами с улучшенными характеристиками и широкими функциональными возможностями.

Основными характеристиками телекамер являются:

1. Оптический формат – размер фоточувствительной области ПЗС-матрицы в дюймах.

2. Разрешающая способность (разрешение) – максимальное количество телевизионных линий (ТВЛ), различаемых визуально в выходном сигнале камеры при минимально допустимой глубине модуляции 10 %. Разрешение по горизонтали определяет максимальное количество градаций от черного к белому или обратно, которые могут быть получены от камеры в центральной части экрана.

3. Пороговая чувствительность (чувствительность) – минимальная освещенность на ПЗС-матрице, при которой камера сохраняет работоспособность.

4. Синхронизация – привязка видеосигнала к фазе сетевого напряжения или внешнего источника синхроимпульсов или другого видеосигнала.

5. Электронный «затвор» – элемент электронной части ПЗС-матрицы, обеспечивающий возможность изменения времени накопления электрического заряда (выдержки). Электронный «затвор» позволяет получить приемлемое качество изображения быстродвижущихся объектов и обеспечивает работоспособность камеры в условиях высокой освещенности.

6. Электронная диафрагма (автоматический электронный «затвор», электронный ирис) – элемент электронной части ПЗС-матрицы, обеспечивающий автоматическую регулировку выдержки в зависимости от уровня освещенности.

7. Автоматическая регулировка усиления (АРУ) – свойство электронной части камеры изменять коэффициент усиления в видеотракте в зависимости от уровня видеосигнала. АРУ сглаживает изменения уровня сигнала и позволяет получить приемлемую «картинку» на мониторе при недостаточной освещенности объекта.

8. Отношение сигнал/шум. Позволяет учитывать, когда требуется высокое качество телевизионного сигнала – чем оно выше, тем выше качество изображения.

9. Автоматический баланс белого (для цветных камер) – способность камеры обеспечивать правильную цветопередачу при изменении условий освещенности наблюдаемых объектов.

Объектив – это устройство, формирующее изображение объекта в плоскости ПЗС-матрицы. Он может быть встроенным или сменным.

Фокусное расстояние f (мм) – характеризует величину угла зрения при определенном оптическом формате камеры.

Трансфокатор – устройство, позволяющее изменять фокусное расстояние в широких пределах (ZOOM- функция).

Относительное отверстие F определяет освещенность на ПЗС-матрице.

По конструктивному признаку телевизионные камеры можно подразделить на корпусные и бескорпусные. Бескорпусные камеры имеют значительно меньшие габариты и стоимость по сравнению с камерами в корпусе и предназначены для систем скрытого наблюдения. Камеры для открытого внутреннего наблюдения размещаются в защитных корпусах (кожухах), которые имеют разную форму (сфера, полусфера и т. д.), габариты, конструкцию крепления (потолочная, настенная, угловая) и позволяют выбрать оформление, наиболее подходящее к конкретному интерьеру. Камеры для использования на открытом воздухе помещаются в защитные кожухи, оборудованные подогревом – термокожухи. Термокожухи предназначены для работы в широком диапазоне климатических условий и позволяют использовать различные комбинации телекамер и объективов. Кожух снабжен солнцезащитным козырьком (либо фильтром), платой для установки камеры, термостатом и коммутационной панелью. Некоторые термокожухи имеют дополнительное оборудование – вентиляторы, дворники, омыватели стекла.

Поворотные устройства предназначены для телекамер с дистанционным управлением. Они обеспечивают поворот в горизонтальной (до ±365°) и в вертикальной (до ±183°) плоскостях либо только в горизонтальной.

Как правило, вместе с поворотными устройствами поставляются пульты управления, с помощью которых можно манипулировать также трансфокаторами объективов, если требуется получить укрупненное изображение.

Рассмотрим программное обеспечение «КОДОС-ВИДЕОСЕТЬ», версия 5.0, используемое для организации системы видеонаблюдения в данной лабораторной работе.

Видеонаблюдение осуществляется видеокамерами, которые подключают:

1) к серверу системы видеонаблюдения «КОДОС-ВИДЕОСЕТЬ»;
2) по локальной сети или сети Internet.

Камеры подключаются к компьютеру через следующее оборудование:

- платы видеоввода;
- порты USB;
- локальную сеть или Internet – для IP-камер.

Работа системы видеонаблюдения «КОДОС-ВИДЕОСЕТЬ» возможна в следующих конфигурациях:

1) путем подключения аналоговых камер к платам видеоввода;
2) путём подключения IP-камер по сети Ethernet.

Допускается построение систем комбинированного типа (аналоговые камеры + IP-камеры).

В любом случае в системе может быть несколько серверов и несколько приёмников, соединённых по сети Ethernet. Также к системе может подключаться дополнительное оборудование (микрофоны, поворотные устройства).

Подключение видеоплат и установка драйверов описана в документации на эти устройства.

Возможности видеоплат по преобразованию аналогового сигнала в цифровой зависят от мощности компьютера, параметров видео (количество кадров в секунду, разрешение, цвет) и пропускной способности локальной сети.

«КОДОС-ВИДЕОСЕТЬ» обрабатывает изображение с аналоговых видеокамер, подключенных к платам видеозахвата, IP-видеокамер, IP-видеохабов. USB видеокамер. Аналоговые камеры передают аналоговый сигнал на плату видеозахвата, где он оцифровывается. IP-камера имеет схему цифровой обработки, компрессии и передачи изображения. Оно передается от такой камеры в сеть Internet или LAN. Каждая камера имеет IP-адрес и встроенное программное обеспечение, что позволяет ей функционировать в качестве web-сервера.

USB камера передает изображение через USB-порт.

Производительность видеосервера системы оценивают в суммарном числе кадров в секунду, которые способен обработать сервер и в числе кадров в секунду для одного канала. При этом скорость захвата-отображения на экране, скорость записи в архив и скорость передачи по сети могут быть разными. Например, плата видеозахвата захватывает «живое» видео со скоростью 25 кадров в секунду, на экран отображается тоже 25 кадров в секунду, скорость записи в архив установлена 8 кадров в секунду, а по сети удаленному клиенту по медленному каналу передается один кадр в секунду. Максимальная скорость захвата и отображения видео ограничивается полосой пропускания шины PCI и определяется следующими факторами:

- цветность изображения;
- разрешение изображения.

Цветное изображение занимает в два раза больше места, чем черно-белое и, соответственно, скорость его захвата, сжатия и передачи по сети значительно ниже.

Платы видеозахвата, оцифровывающие сигнал с видеокамер, выдают строго определенный набор разрешений, заданный форматом видеосигнала PAL. Полный кадр видеосигнала имеет разрешение 768 × 576. При этом он формируется из двух полей, каждое из которых имеет разрешение 768 × 288. Поля содержат «чересстрочную» информацию – «четное» поле содержит четные строки кадра, а «нечетное» – нечетные. Если происходит съемка движущегося объекта, то изображение в этих двух полях оказывается смещенным и при их сложении в полный кадр образуется эффект «гребенки». Таким образом, для получения полного кадра 768 × 576 видеосистема должна сложить два поля и при помощи математического алгоритма устранить эффект гребенки.

Программное обеспечение «КОДОС-ВИДЕОСЕТЬ» позволяет записывать в архив «живое» видео с той же скоростью, с которой изображение отображается на экране. Эта возможность ограничивается только мощностью процессора. Но для большинства случаев нет необходимости записи видео с такой скоростью, поскольку для этого требуется более мощный сервер и большой размер дисков. Исходя из опыта считается, что скорость 4 кадра в секунду вполне достаточной для анализа ситуаций по видеоархиву, а скорость 8 кадров в секунду при просмотре архива равносильна «живому» видео. По умолчанию для всех каналов устанавливается скорость записи в архив 4 кадра в секунду.

ПО «КОДОС-ВИДЕОСЕТЬ» предлагается использовать три алгоритма сжатия видеопотока – «SSA быстрый». «SSA медленный» и «SSA смешанный», с различными опциями.

По умолчанию на сервере устанавливается алгоритм сжатия «SSA быстрый, адаптивный», с опорными кадрами, качество «95 %». Это эффективный алгоритм компрессии с «wavelet» преобразованием и использованием механизма опорных кадров по аналогии с алгоритмами MPEG, но при этом более быстрый. Для большинства задач это идеальный вариант.

Программа «КОДОС-ВИДЕОСЕТЬ» используется для анализа обстановки в местах наблюдения. Для этого совместно используются детекторы движения и детекторы звука. Это позволяет повысить надежность анализа, сократить время для принятия решения при возникновении опасных ситуаций. Детектор движения проводит анализ изображения, детектор звука – анализ звука.

Детектор движения – это элемент программы, анализирующий изображение. Если обнаруживается движение, то детектор может включить запись и/или изменить скорость записи изображения.

Детектор движения имеет широкий диапазон настроек, позволяя пользователю выбрать оптимальные условия работы. Индивидуально настраивается размер и положение зон контроля, чувствительность и другие.

Изображение, видимое на мониторе, можно условно разделить на области. Наиболее информативны те, в которых возможно движение. Но и само движение может быть разным по темпу. Например, нарушитель может бежать, ползти, медленно перемещаться. Поэтому области, в которых темп движения не изменяется, можно объединить в зоны и назначить им одинаковые параметры детектора. Основными параметрами каждой зоны являются чувствительность и порог срабатывания. Количество зон и областей, их положение и размер задаются пользователем.

Принцип работы детектора движения основан на постоянном сравнении соседних видеокадров: предыдущего и текущего. Изображение состоит из так называемых «фасет». Сработавшими считаются те фасеты, в которых зафиксировано изменение больше заданного.

«Чувствительность» – параметр, позволяющий настроить минимальное изменение фасеты, при котором фасета будет признана сработавшей. Данный параметр измеряется в относительных величинах, поэтому настройку следует производить, учитывая условия видеонаблюдения и помехозащищенность видеосигнала.

«Порог срабатывания» – параметр, позволяющий настроить минимальное число сработавших фасет, которое будет приводить к срабатыванию детектора движения. Значение этого параметра подбирается опытным путем, учитывая при подборе параметры видеокамеры, объектива, освещения и т. д. Также на разных участках одного кадра могут перемещаться объекты разной величины – например, пешеход и автомобиль.

Для исключения помех от определенных зон кадра используется редактирование зон. Каждой зоне отдельно задаются размеры, параметры чувствительности и порога срабатывания.

Одним из назначений программы «КОДОС-ВИДЕОСЕТЬ» является сохранение видеоинформации в виде архивных записей на жестком диске ПК. Но постоянная запись ведет к быстрому заполнению жестких дисков, поэтому программа предполагает включение записи в архив в некоторых случаях:

- по команде оператора;
- по расписанию;
- по срабатыванию детекторов движения и звука;
- по срабатыванию тревожного датчика.

При любом из этих вариантов включения канала на запись, происходит задержка во времени, вследствие которой может произойти потеря информации.

Часто бывает важно зафиксировать несколько мгновений, предшествовавших событию включения записи. Для этого и создана предтревожная запись. При подаче команды на запись программа вначале заархивирует содержимое буфера, затем – кадры текущего изображения, до команды остановки записи в архив.

В настройках видеоканалов плат «КОДОС V4» и «КОДОС V16» есть возможность включать предтревожную запись установленного количества кадров с различной частотой. Например, сначала с установленной для данного канала скоростью сжатия, а затем – с установленной при редактировании детектора движения.

В программе «КОДОС-ВИДЕОСЕТЬ» предусмотрен «Режим повышенной бдительности», позволяющий выводить на экран монитора только те окна, на которых зафиксировано движение. При отсутствии движения на экран будут выведены все видеоканалы в заданной конфигурации.

ОПИСАНИЕ ЛАБОРАТОРНОГО СТЕНДА

Конфигурация системы задается структурной схемой, приведенной на рис. 5.1.

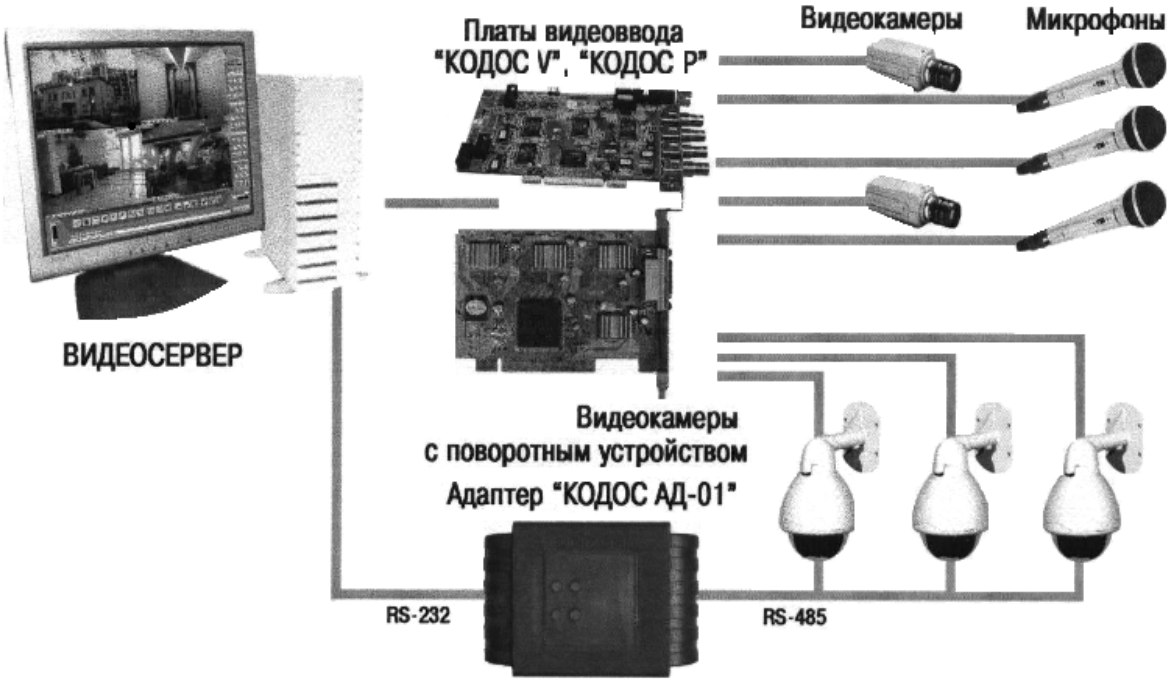

Рис. 5.1. Структурная схема системы видеонаблюдения

В состав лабораторного стенда входят следующие устройства:

- автоматизированное рабочее место;
- плата видеоввода « КОДОС V»;
- видеокамеры;
- адаптер «КОДОС АД-01»

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Изучить общие положения построения систем видеонаблюдения.
2. Ознакомиться со структурной схемой, назначением модулей и их подключением.
3. Ознакомиться с техническими характеристиками устройств и условиями их эксплуатации.
4. Составить проект системы.
5. Выполнить монтаж схемы и подключение устройств.
6. Подготовить систему к запуску.

Прежде, чем приступить к эксплуатации системы, необходимо тщательно изучить и произвести все необходимые настройки в точном соответствии с прилагаемыми описаниями и документацией.

7. Проверить настройки и работоспособность системы видеонаблюдения.

Проверка правильности выполненных монтажных работ проводится в виде тестовых испытаний (в различных режимах) и визуального наблюдения реакции системы на происходящие события.

Основной причиной неработоспособности системы является несоблюдение полярности при подключении устройств. Перечень возможных неисправностей и способов их устранения приведены в документации на соответствующие устройства.

8. Ответить на контрольные вопросы.
9. Подготовить отчет.

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Назовите основные особенности применения системы видеонаблюдения при срабатывании сигнала тревоги.
2. Перечислите компоненты системы телевизионного наблюдения.
3. Основные параметры, характеристики телевизионных камер и их конструктивные признаки.
4. Параметры современных объективов.
5. Возможные конфигурации работы системы видеонаблюдения «КОДОС-ВИДЕОСЕТЬ».
6. Раскройте принципы работы системы «КОДОС-ВИДЕОСЕТЬ» в режиме «детектор движения».
7. В чем заключается назначение основных компонентов моделируемой системы видеонаблюдения?

Список литературы

1. Шакиров Ф.А. Системы телевизионного наблюдения. – М.: НОУ «Такир», 1998. – 56 с.
2. Плата видео/аудио вывода «КОДОС V4»: руководство по эксплуатации. – М.: Изд-во НПК «СоюзСпецАвтоматика», 2008. – 16 с.
3. Адаптер RS-232/RS-485 «КОДОС АД-01»: руководство по эксплуатации. – М.: Изд-во НПК «СоюзСпецАвтоматика», 2008. – 14 с.
4. Рольф М. Основы построения систем охранной сигнализации / пер. с англ. N Н-10736. – М.: ВЦП, 1984. – 71 с.
5. 0мельянчук А.М. Применение видеотехники в охране. – М.: ТВ «Безопасность», 1995. – 72 с.
6. Никулин О.Ю., Петрушин А.Н. Системы телевизионного наблюдения. – М.: «Оберег-РБ», 1997. – 176 с.
7. Настоящее и будущее CCTV // Системы безопасности. – 1995, № 6. – С. 62–63.
8. Крыжановский В.Д., Костыков Ю.В. Телевидение цветное и ТВ «черно-белое». – М.: «Связь», 1990.
9. Демин Ю.И., Петраков А.В. Современные автоматизированные охранные системы: тезисы докладов на НТК МТУСИ. – 1993. – С. 9–10.

Учебное издание

СТЕПАНОВ Борис Павлович

ТЕХНИЧЕСКИЕ СРЕДСТВА СИСТЕМ БЕЗОПАСНОСТИ И ПРОТИВОДЕЙСТВИЯ ЯДЕРНОМУ ТЕРРОРИЗМУ

Методические указания к выполнению лабораторных работ
по курсу «Безопасность эксплуатации ядерных энергетических установок»
для магистрантов, обучающихся по специальности
«Физико-технические проблемы атомной энергетики»
направления 010700 «Физика»

Научный редактор
доктор физико-математических наук,
профессор — *И.В. Шаманин*

Редактор — *С.П. Барей*

Верстка — *В.П. Аршинова*

Дизайн обложки — *О.Ю. Аршинова*
О.А. Дмитриев

Подписано к печати 17.12.2008. Формат 60x84/16. Бумага «Снегурочка».
Печать XEROX. Усл. печ. л. 2,33. Уч.-изд. л. 2,1.
Заказ 888. Тираж 100 экз.

Томский политехнический университет
Система менеджмента качества
Томского политехнического университета сертифицирована
NATIONAL QUALITY ASSURANCE по стандарту ISO 9001:2000

ИЗДАТЕЛЬСТВО ТПУ. 634050, г. Томск, пр. Ленина, 30.