

Рыжова В.А., Горбачев А.А., Коротаев В.В.

ОПТИКО-ЦИФРОВЫЕ СИСТЕМЫ



**Санкт-Петербург
2018**

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

Рыжова В.А., Горбачев А.А., Коротаев В.В.

Оптико-цифровые системы

**УЧЕБНОЕ ПОСОБИЕ
ПО КУРСОВОМУ ПРОЕКТИРОВАНИЮ**

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УНИВЕРСИТЕТЕ ИТМО
по направлению подготовки 12.04.02 «Оптотехника» в качестве учебного
пособия для реализации основных профессиональных образовательных
программ высшего образования магистратуры



**Санкт-Петербург
2018**

Рыжова В.А., Горбачев А.А., Коротаев В.В. Оптико-цифровые системы. Учебное пособие по курсовому проектированию. – СПб.: Университет ИТМО, 2018. – 95 с.

Рецензент: Арбузов С.Н., к.ф.-м.н., бренд-менеджер ООО «Легарда»

Учебное пособие предназначено для студентов по направлению подготовки магистратуры 12.04.02 «Оптотехника». Представлены тематика курсового проектирования, содержание и методика выполнения курсового проекта, список стандартов и руководящих документов для выполнения работ по формированию пояснительной записки и графических материалов по проектированию оптико-цифровых систем для обеспечения комплексной безопасности объектов. Методика выполнения курсовых проектов разработана с использованием учебной и специальной научно-технической литературы по проектированию комплексных автоматизированных систем безопасности, а также типовых методических материалов по курсовому проектированию.



Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

© Университет ИТМО, 2018

© Рыжова В.А., Горбачев А.А., Коротаев В.В. 2018

Содержание

ВВЕДЕНИЕ	4
1. Общие положения	5
2. Тематика курсового проекта и организация его выполнения	7
3. Содержание курсового проекта	9
4. График выполнения курсового проекта.....	13
5. Методика курсового проектирования	16
5.1. Проведение предпроектного обследования.....	16
5.2. Разработка концепции и технического задания на создание системы безопасности.....	24
5.3. Разработка проектных решений.....	28
5.3.2 Порядок проектирования охранно-пожарной сигнализации.....	29
5.3.2 Порядок проектирования системы охранного телевидения.....	45
5.3.3 Порядок проектирования системы контроля и управления доступом.....	67
5.4. Определение элементов интеграции оптико-цифровых систем при проектировании комплексной системы безопасности объекта	82
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....	85
ПРИЛОЖЕНИЕ 1	88
ПРИЛОЖЕНИЕ 2	90

ВВЕДЕНИЕ

Курсовой проект выполняется студентами кафедры оптико-электронных приборов и систем (ОЭПиС), обучающимися по направлению подготовки магистров 12.04.02 «Оптотехника» в рамках магистерской программы «Оптико-электронные цифровые системы», в течение первого семестра.

Учебно-методическое пособие предназначено для студентов кафедры ОЭПиС. Даются рекомендации по выбору тематики и содержанию курсового проекта по дисциплине «Оптико-цифровые системы», его оформлению и защите. Методические указания составлены с учетом следующих инструктивных материалов:

1. Образовательный стандарт высшего образования Санкт-Петербургского национального исследовательского университета информационных технологий, механики и оптики. Уровень высшего образования Магистратура. Направление подготовки 12.04.02 Оптотехника. Квалификация Магистр. – Принят Ученым Советом НИУ ИТМО 28.01.2014. Протокол №1 – СПб, 2014. – Электронный ресурс: <http://edu.ifmo.ru/file/pages/104/12.04.02.pdf>.
2. Положение о проведении текущего контроля успеваемости и промежуточной аттестации студентов НИУ ИТМО. – Одобрено Ученым советом университета 28.02.2012. Протокол №2 –СПб, 2012. – Электронный ресурс: http://edu.ifmo.ru/file/pages/109/4_polozhenie_o_provedenii_tekushego_kontrolya.pdf
3. Рекомендации по организации проведения курсового проектирования в СПбГУ ИТМО – СПб, 2009. – Электронный ресурс: http://edu.ifmo.ru/file/pages/211/rekomendacii_po_organizacii_provedeniya_kursoвого_projektirovaniya.pdf

1. Общие положения

Курсовое проектирование (КП) представляет собой вид учебной работы по дисциплине «Опτικο-цифровые системы» и выполняется в пределах часов, отводимых на ее изучение. КП представляет собой форму самостоятельной работы, цель которой заключается в подготовке магистранта к выполнению выпускной квалификационной работы.

Задачами КП являются:

- систематизация (обобщение), закрепление и расширение (углубление) теоретических и практических знаний по изучаемой дисциплине;
- закрепление умений применять полученные знания при решении конкретных типовых и нестандартных задач;
- развитие творческого мышления и навыков самостоятельной работы;
- приобретение навыков проектирования систем на основе совместных действий в команде;
- приобретение опыта аналитической, расчетной работы и формирование соответствующих умений;
- приобретение навыков использования справочной, нормативной и научной литературы, а также Интернет-ресурсов;
- приобретение навыков оформления пояснительной записки;
- формирование умения грамотно составить доклад для защиты проекта;
- формирование умений выступать перед аудиторией с докладом при защите проекта, компетентно отвечать на вопросы, вести профессиональную дискуссию, убеждать оппонентов в правильности принятых решений.

За актуальность, соответствие тематики КП целям и задачам дисциплины, а также организацию его выполнения несет ответственность руководитель КП. Руководитель КП:

- корректирует и утверждает задание на КП;
- оказывает студенту помощь в организации и выполнении КП;
- проводит систематические плановые занятия со студентом и консультирует его;
- выполняет поэтапную проверку курсового проекта в рамках текущей аттестации;
- оценивает своевременность и качество выполнения курсового проекта в рамках промежуточной аттестации.

За все сведения, изложенные в курсовом проекте, принятые решения и за правильность всех данных ответственность несет непосредственно студент – автор курсового проекта.

Завершенный курсовой проект (пояснительная записка, графические материалы), подписанный студентом, представляется руководителю для оценки.

Руководитель проверяет соответствие выполненного проекта заданию. Руководитель дает общую оценку работы по четырехбалльной шкале (отлично, хорошо, удовлетворительно, неудовлетворительно) и по общеевропейской шкале (A, B, C, D, E). Основаниями для снижения оценки являются:

- небрежное выполнение;
- низкое качество графического материала;
- невозможность студента объяснить полученные результаты.

Материалы КП не могут быть приняты и подлежат доработке в случае:

- отсутствия необходимых разделов;
- отсутствия необходимого графического материала;
- присутствия грубых ошибок при расчетах;
- отсутствие обоснования выбора компонентов систем;
- несвоевременное выполнение этапов задания.

Руководитель обязательно учитывает соответствие представленных проектных решений современному уровню развития науки и технологий, степень самостоятельности и творческого участия студента в работе над курсовым проектом.

2. Тематика курсового проекта и организация его выполнения

Тематика КП ориентирована на формирование специализированной оптико-цифровой системы, направленной на поддержание безопасного состояния объектов различного назначения, предупреждение, обнаружение, противодействие и ликвидацию угроз жизни, здоровью и среде обитания граждан, их имуществу и информации.

Выбор указанной тематики соответствует требованиям Правительства РФ по обеспечению антитеррористической защищенности объектов (территорий) практически во всех сферах жизнедеятельности граждан, включая вопросы инженерно-технической укрепленности объектов охраны, их оснащённости современными аппаратно-техническими и программными средствами.

Курсовой проект предполагает постановку задач проектирования автоматизированной оптико-цифровой комплексной системы безопасности (КСБ) для объекта охраны с элементами интеграции формирующих ее подсистем, формулировку и анализ проблемной ситуации, разработку технического предложения, содержащего рассмотрение нескольких возможных путей ее разрешения, обоснование избираемого варианта решения, составление технического задания на проект, выполнение расчетных, проектных этапов, включая обязательную разработку комплекта или отдельных элементов технической документации.

Структура задания на курсовое проектирование предполагает наличие ряда разделов следующего содержания.

В разделе "Тема проекта" формулируется точное название разрабатываемой системы.

В разделе "Техническое задание" должны быть приведены:

- а) подробное и конкретное назначение системы;
- б) технические требования к проектируемой системе (режим функционирования, размещение блоков, способы регистрации, обработки, хранения и передачи получаемой информации и пр.);
- в) исходные данные для расчета основных параметров и характеристик компонентов системы;
- г) условия эксплуатации;
- д) указание на источник питания;

По отдельным исходным данным допускается указание: "Уточняется в процессе разработки".

В разделе "Содержание пояснительной записки" указываются все подлежащие разработке вопросы. В содержание КП могут быть включены задачи создания элементов готовой продукции (например, коммерческого предложения на систему обеспечения комплексной безопасности объекта охраны). Примерное содержание и формулировка разделов пояснительной записки приведены в типовом задании (см. Приложение 1).

В разделе "Перечень графического материала" указываются обязательно представляемые планы и схемы и их объем. К ним относятся разработанные студентом план объекта охраны, структурная схема системы, план размещения оборудования, а также при необходимости схемы, поясняющие соединение отдельных функциональных узлов.

В разделе "Исходные материалы и пособия" приводится рекомендуемая руководителем литература.

Для развития инициативного подхода к решению задач проектирования систем безопасности реализуется технология обучения в сотрудничестве. Формируются группы учащихся по 3-4 человека для реализации проектного задания. Эффективность работы в команде определяется способностью каждого члена группы самостоятельно приобретать и использовать с помощью информационных и компьютерных технологий новые знания и умения при выполнении своей части задания, а также совместными действиями по выработке технически обоснованного варианта построения КСБ для объекта охраны.

Результатом выполнения КП является приобщение студентов к отработке основных этапов концептуального и рабочего проектирования систем безопасности, расчету и выбору основных параметров и характеристик охраняемых систем, к анализу режима функционирования интегрированной системы в целом.

Проверка этапов выполнения заданий осуществляется на каждом практическом занятии в виде коллективных обсуждений результатов работы студенческих групп, проведения дискуссий, ролевых игр, повышающих степень вариативности при поиске наиболее приемлемого решения поставленной задачи.

3. Содержание курсового проекта

В рамках курсового проектирования каждый из участников инициативной группы учащихся занимается разработкой или реинжинирингом функциональной подсистемы автоматизированной КСБ объекта с учетом его назначения, категории, структуры, специфики работы и местоположения. Проектируются следующие функциональные подсистемы безопасности (ПСБ) объекта:

- система охранной сигнализации (СОС);
- система пожарной сигнализации (СПС);
- системы тревожной сигнализации (СТС);
- система контроля и управления доступом (СКУД);
- система охранного телевидения (СОТ).

В качестве учебного объекта могут рассматриваться предприятия промышленной, финансовой, медицинской, образовательной, торговой, транспортной сфер, жилищные комплексы.

Объект охраны выбирается каждой группой студентов самостоятельно или может предлагаться руководителем из следующего списка:

- аптечная сеть (5 аптек по 3-5 помещений, площадью до 350 кв.м) с центральным офисом и складом (площадью 400 кв.м);
- сеть из пяти автозаправочных станций (АЗС) площадью по 300-800 кв.м (автомойка, магазин, служебные помещения) с центральным офисом (кабинет директора, бухгалтерия, служебные помещения);
- складской комплекс (одноэтажный, высота потолков 7-10 м), содержащий один ангар (площадь 2000 кв.м, потолок 10 м), три здания складов (площадью по 700 кв.м), одно офисное здание (двухэтажное по 10 помещений на каждом этаже);
- бизнес-центр (3 трехэтажных корпуса площадью по 5000 кв.м), корпуса соединены переходами;
- бизнес-центр (одно здание на 7 этажей) общей площадью 10 000 кв.м, по 15-20 помещений на каждом этаже;
- коттедж (3 этажа) с прилегающей территорией и постройками (баня, отдельно стоящий гараж, гостевой домик) – общая площадь помещений 400 кв.м, цокольный этаж (бойлерная, бассейн);
- торговый гипермаркет общей площадью 3000 кв.м с прилегающей территорией - торговая зона (2000 кв.м), складские и служебные помещения, парковка (150×200 м) с контролем въезда/выезда через шлагбаум (или со свободным въездом);
- автопарк общей площадью 6000 кв.м (огороженная открытая парковка – шлагбаум на въезд/выезд, офис до 300-400 кв.м, ремзона, склады запчастей, сейф для хранения выручки);
- многоквартирный дом на 17 этажей с паркингом.

Структура предлагаемых объектов не является жестко регламентированной. Состав и параметры объектов окончательно утверждаются на втором практическом занятии, когда каждая группа составляет (или выбирает на основе проведенного информационного поиска) и предоставляет для обсуждения план объекта.

Все системы охраны должны закладываться с учетом дальнейшего расширения и модернизации (например, не все помещения заселены, планируется привлечение арендаторов и прочие условия для возможности развития системных решений). В процессе курсового проектирования студент должен выполнить ряд действий:

1. Провести предпроектное обследование и анализ уязвимости учебного объекта.
2. Формализовать результаты предпроектного обследования в виде комплекса потенциальных угроз и возможных рисков.
3. Выполнить постановку задачи на проектирование функциональной подсистемы интегрированной КСБ.
4. Спроектировать структуру и схему расположения оборудования.
5. Разработать элементы аппаратного и программного обеспечения функциональной ПСБ.
6. Разработать проектную документацию на функциональную подсистему.
7. Оформить пояснительную записку и графическую часть проекта.

Каждый участник проектной группы ведёт информационный поиск оборудования и программного обеспечения для своей ПСБ в рамках актуального ассортимента, представленного на рынке безопасности Санкт-Петербурга, с учетом необходимых параметров и цен. В итоге совместной деятельности группы к защите должна быть представлена пояснительная записка, содержащая подробное описание работы составных частей КСБ и организацию их взаимодействия.

Пояснительная записка состоит из введения, основной части, заключения, списка использованных источников и приложения. Список использованных источников составляется в соответствии с требованиями к оформлению библиографии.

Материалы в пояснительной записке следует располагать в следующем порядке:

- титульный лист;
- задание на проектирование;
- содержание;
- введение (формулируется актуальность формирования КСБ для учебного объекта, цели и задачи проектирования);
- общая часть (формируется концепция создания системы, в которой указываются общие цели, задачи и требования к составу и взаимодействию составных частей системы; составляется

техническое задание на проектирование системы, в котором описывается существующее положение на основе результатов предпроектного обследования объекта и анализа его уязвимости, с указанием перечня нормативных и руководящих документов, в соответствии с которыми выполняется рабочий проект);

- проектные решения (проводятся выбор и обоснование локальных зон контроля, состав локального и центрального пунктов наблюдения, структура и планы размещения оборудования для каждой функциональной ПСБ, требования по электропитанию);
- технико-экономический расчет (составление видоизмененной спецификации, описывающей количественные и ценовые характеристики оборудования и расходных материалов для монтажа функциональной ПСБ и интегрированной КСБ в целом на объекте охраны);
- заключение (выводы по проекту, возможности дальнейшего масштабирования и усовершенствования системы);
- список использованных источников;
- приложения (планы, схемы, результаты расчетов, рисунки, анкеты, опросные листы, подготовленные для предпроектного обследования объекта).

Пояснительная записка оформляется в соответствии с требованиями, предъявляемыми к оформлению научных работ (см. Приложение 2). Объем пояснительной записки курсового проекта может составлять 30-40 страниц.

В пояснительной записке должны быть выдержаны единые обозначения и единые размерности для используемых параметров. Допускаются только общепринятые сокращения слов, терминов, обозначений. Законченная пояснительная записка подписывается студентом и руководителем проекта. Изложение должно быть ясным и четким, без повторений, количество иллюстраций - минимальным, но достаточным для пояснения изложенного.

Графическая часть курсового проекта включает:

1. План объекта обеспечения безопасности с указанием размеров и необходимых видов.

2. Структурная схема функциональной ПСБ.

3. План размещения оборудования для функциональной ПСБ.

4. Спецификация оборудования для функциональной ПСБ.

Графическая часть проекта является не иллюстративным материалом, а технической документацией на разработанный студентом проект ПСБ.

Структурная схема отображает количественный состав, взаимодействие основных элементов разрабатываемой ПСБ, тип соединений между ними, а также определяет каналы связи для передачи тревожных извещений.

План размещения оборудования для каждой ПСБ предполагает

указание поэтажного расположения технических средств обнаружения угроз в соответствии с установленными размерами и характеристиками уязвимости блокируемых участков (открывание, пролом, перелаз, подкоп, разбитие, комбинация способов). Указывается расстояние от его составных частей оборудования до строительных конструкций помещения с нанесением установочных размеров.

Необходимо выделить помещения выдачи сигналов тревоги, отобразить места размещения технических средств ССОИУ (центрального пульта наблюдения, АРМ операторов системы, контрольных панелей, мониторов наблюдения и тревоги, контроллеров, считывателей, световых и звуковых оповещателей, преграждающих устройств, устройств записи, хранения и воспроизведения информации).

Графический материал следует размещать в приложениях. Графический материал по формату, условным обозначениям, шрифтам и масштабам должен соответствовать требованиям единой системы конструкторской документации и руководящих документов по проектированию систем безопасности (см. Приложение 2).

4. График выполнения курсового проекта

Согласно рабочей программе дисциплины, на выполнение курсового проекта отводится семестр с защитой в рамках зачетной сессии. Контроль выполнения КП осуществляются на каждом этапе (критерии для текущего контроля приведены в таблице 1). В ходе контактной работы с инициативной группой студентов руководитель КП рассматривает промежуточные результаты проектирования и при необходимости осуществляет коррекцию направления разработки.

Таблица 1– График выполнения курсового проекта

№ п/п	Наименование этапа	Продолжительность этапа, % от общей трудоемкости КП	Критерии оценивания
1	Формирование задания на курсовой проект. Выбор плана учебного объекта. Составление технического задания на проектирование функциональной ПСБ.	20	способность применять современные методы исследования, знание особенностей формирования архитектуры и состава современных оптико-цифровых систем для решения задач комплексной безопасности объектов; владение навыками определения порядка выполнения работ с использованием современных информационных технологий
2	Поиск и анализ информационных источников для обоснования основных проектных решений.	20	способность к анализу состояния научно-технической проблемы, технического задания и постановке цели и задач проектирования оптико-цифровых систем, владение навыками обоснованного выбора основных компонентов и элементов проектируемой системы с использованием информационных ресурсов

№ п/п	Наименование этапа	Продолжительность этапа, % от общей трудоемкости КП	Критерии оценивания
3	Выполнение расчетно- графической части проекта.	20	способность к проведению технических расчетов и функционально-стоимостн ому анализу эффективности проектируемых систем, владение навыками расчета параметров элементов систем безопасности, объёмов памяти для хранения данных, а также сметной стоимости основного, дополнительного оборудования и расходных материалов.
4	Формирование функциональной ПСБ и интегрированной оптико-цифровой КСБ в целом.	20	способность к разработке структурных схем оптико-цифровых систем с установлением технических требований на отдельные блоки, владение методикой выбора варианта охраны объекта и комплекса аппаратно-программных средств обеспечения безопасности в соответствии с требованиями к укрепленности объекта
5	Анализ результатов проекта. Оформление пояснительной записки и графических материалов.	10	способность оценивать результаты выполненной работы, умение выполнять основные этапы проектирования оптико-цифровых систем безопасности с элементами интеграции их элементов

№ п/п	Наименование этапа	Продолжительность этапа, % от общей трудоемкости КП	Критерии оценивания
6	Защита курсового проекта	10	способность представлять результаты выполненной работы, умение ориентироваться в современных аппаратно-программных средствах обеспечения безопасности.

Руководитель проводит поэтапный контроль и итоговое оценивание (в ходе защиты) результатов выполнения курсового проекта.

5. Методика курсового проектирования

5.1 Проведение предпроектного обследования

Целью предпроектного обследования в рамках учебного проектирования является формирование концепции создания оптико-цифровой КСБ с элементами интеграции составляющих ее подсистем и технического задания (ТЗ) на ее разработку.

Основная задача обследования – изучение существующего положения на учебном объекте, анализ уязвимости объекта, а также оценка реального объема проекта по созданию КСБ, ее целей, задач, состава и взаимодействия функциональных подсистем.

Анализ уязвимости учебного объекта проводится с целью определения приоритетных объектов защиты, рассмотрения вариантов возможных угроз и моделей их реализации для разработки проектных решений по усилению безопасности объекта [1, 4-7].

Для различных предприятий, в зависимости от особенностей профиля деятельности, существует различный набор ресурсов и соответствующие им прогнозируемые угрозы безопасности. Важными для жизнедеятельности ресурсами, а, следовательно, объектами защиты являются:

- люди (персонал предприятия);
- имущество;
- технологическое оборудование;
- материальные и финансовые ценности;
- готовая продукция;
- интеллектуальная собственность (ноу-хау);
- конфиденциальная информация на материальных носителях, а также циркулирующая во внутренних коммуникационных каналах связи, в кабинетах руководства предприятия, на совещаниях и заседаниях;
- финансово-экономические ресурсы, обеспечивающие эффективное и устойчивое развитие предприятия (капитал, коммерческие интересы, бизнес-планы, кадровая статистика, договорные документы и обязательства и т.п.).

Основными угрозами, которые могут привести к значительному урону, являются:

- чрезвычайная ситуация (пожар, разрушение, затопление, авария);
- хищение опасных веществ и т.п.;
- хищение или порча имущества;
- несанкционированный съем конфиденциальной информации из защищаемых помещений.

Реализация перечисленных угроз может привести:

- к созданию угрозы для жизни и здоровья людей;
- к катастрофическим последствиям для окружающей среды и населения;

- к большому материальному ущербу;
- к разглашению конфиденциальной информации или сведений, содержащих коммерческую тайну;
- к банкротству предприятия.

При проведении предпроектного обследования в первую очередь нужно охарактеризовать исследуемый объект с точки зрения его уязвимости, то есть степени несоответствия существующих мер защиты прогнозируемым угрозам или заданным требованиям безопасности.

Характеристику объекта рекомендуется составлять, придерживаясь следующей последовательности признаков, влияющих на безопасность:

- архитектурно-планировочные решения объекта (этажность, размеры, наличие внутренних территорий и искусственных препятствий в виде ограждений и т.п. сооружений);
- место расположения объекта с учетом географических особенностей и степени изолированности зданий (если это сельская местность или пригород);
- возможность использования природных факторов защиты, например рек, водохранилищ, гор и др.;
- существующий или потенциальный уровень и характер преступности в данном месте или районе (например, кражи со взломом, просто кражи, ДТП, вандализм и т.д.);
- близость к местам массового скопления народа (стадион, аэропорт, дискотеки, пансионат, гостиницы и др.);
- природные и погодные условия, времена года, или сезонные факторы, например потоков туристов;
- степень удаленности необходимых служб (милиция, скорая помощь, пожарные);
- особенности организации уличного и дежурного освещения;
- фактор видимости, т.е. расстояние, с которого видно соседний объект.

Кроме вышеперечисленных факторов, при описании объекта необходимо учитывать возможное несанкционированное проникновение с помощью средств обслуживания, например грузовые лифты, места хранения подсобных материалов, вентиляционные люки, мусоропроводы и др. При приеме посетителей необходимо создавать специальные зоны, где они могут получить необходимую информацию. Операционные стойки должны обеспечивать персоналу обзор этих зон.

Рассмотрение функций и конструкций дверей, окон, запоров это совершенно самостоятельный раздел, напрямую связанный с технической безопасностью объектов, строительными и эстетическими требованиями, которые очень часто бывают взаимно исключаящими.

Потолочные и коммуникационные пустоты также могут быть использованы в преступных целях, поэтому эти площади необходимо

обеспечить защитой. Это может быть физическая защита, препятствующая проходу, или система сигнализации, обнаруживающая проникновение.

Общая стратегия предотвращения краж и поджогов в магазинах и офисах должна рассматривать ситуации, когда помещения открыты для работы и когда они закрыты. Основными направлениями в стратегии должны стать следующие:

- обеспечение условий, при которых потенциальный нарушитель не мог бы проникнуть на объект незамеченным;
- обеспечение освещения, достаточного для наблюдения за действиями нарушителя;
- установка и поддержание в рабочем состоянии запирающих устройств на наружных дверях, окнах и других возможных путях проникновения;
- контроль доступа посетителей в помещения, не предназначенные для посещения клиентов в течение рабочего дня;
- принятие мер к ограничению возможности возникновения пожара с внешней стороны объекта.

Для получения вышеуказанной информации об объекте в реальной практике проектирования КСБ могут быть использованы следующие методы:

- опрос (устный опрос производится при контактной работе с заказчиком проекта по заранее составленному вопроснику с записью ответов; достоинства метода – простота, возможность приступить к подготовке нового решения уже на стадии анализа; недостатки метода – затруднения психологического порядка и разнородность результатов);
- анкетирование заказчика или его представителей (с помощью перечня четких, недвусмысленных вопросов дает полную и основательную информацию при условии готовности опрашиваемых к правдивым ответам; предложение вариантов ответов на каждый вопрос повышает качество анкетирования);
- наблюдение, измерение и оценка (проектная группа собирает и оценивает сведения о параметрах, признаках и объектах в соответствующей предметной области на основе собственных исследований оснащенности объекта и его специфики).

В рамках курсового проектирования группам студентов предлагается выбрать наиболее приемлемый для себя метод для решения задач предпроектного обследования объекта. Рассмотрим метод формирования опросных листов.

Опросный лист позволяет в короткое время получить первичную информацию об объекте охраны и свойствах системы безопасности, которую желает реализовать заказчик. Заказчик не всегда ориентируется в технических особенностях систем безопасности, поэтому вопросы

составляются в терминах, понятных обычному человеку (не специалисту в области систем безопасности).

Ниже приведены наиболее важные вопросы для проектирования функциональных подсистем ОПС и СКУД.

Примерный перечень вопросов для опросного листа по проектированию пожарной, охранной и тревожной сигнализаций

Общие вопросы

1. Вид сигнализации (автономная или с выводом сигнала тревоги на удалённый пульт охраны).
2. Необходимость создания тревожной сигнализации.
3. Необходимость интеграции ОПС с другими системами (системами видеонаблюдения, СКУД, системы контроля технологического процесса, системы контроля утечки воды или газа и пр. системы жизнеобеспечения) и места их расположения.
4. Какие события должны быть обработаны оборудованием функциональных ПСБ, наличие выделенных мест для установки оборудования.
5. Для радиоканальных внутриобъектовых систем необходимо знать материал стен и перекрытий (гипрок, дерево, бетон).
6. Если объект включает несколько зданий, необходимо знать расстояния между ними и наличие средств коммуникации.
7. Наличие на объекте мест возможных подключений различных каналов связи и их расположение.
8. Какие каналы связи существуют для связи с пультом охраны (проводной телефон, GSM, TCP/IP).
9. Определение минимально необходимого количества извещений, передаваемых на пульт охраны (несанкционированное проникновение, пожар, тревожная кнопка и т.п.).
10. Наличие на территории объекта персонала физической охраны. При её отсутствии необходимо уточнить место расположения и удалённость от объекта пульта охраны, который будет реагировать на тревожную информацию.
11. Необходимость создания автоматизированного рабочего места (АРМ) для управления системами ОПС.
12. При наличии на объекте зданий (этажей или помещений) с различными режимами работы (охраны), информация об их расположении и особенностях охраны.

Для пожарной сигнализации

13. Материалы стен, перекрытий, окон, мебели или других горючих предметов.

- 14.Наличие на объекте пожароопасного оборудования (сварочное оборудование или «горячие» цеха, камины, газовые плиты или колонки, бани, газовые котлы и т.п.).
- 15.Наличие на объекте особо опасных предметов или материалов (легковоспламеняющиеся, взрывчатые, ядовитые, радиоактивные.)
- 16.Наличие систем искусственной вентиляции и места расположения (воздухозаборников, кондиционеров и т.п.).
- 17.Высота потолков, расстояния до подвесного потолка при его наличии.

Для охранной сигнализации

- 18.Места нахождения и краткое описание основных ценностей на объекте.
- 19.Материал изготовления дверей (дерево, железо, металлопластик, стекло), одностворчатые или двухстворчатые.
- 20.Материал изготовления окон, наличие форточек или створок (их количество), на каких окнах.
- 21.Наличие нестандартных окон (панорамное или витринное остекление).
- 22.Наличие решеток на окнах, жалюзи.
- 23.Наличие чердаков, люков (места выхода на них).
- 24.Наличие арендаторов или отчужденной территории на объекте заказчика.
- 25.Точность определения места вторжения на объект (возможность объединения различных помещений в один шлейф).
- 26.Места обычного входа на объект пользователями.
- 27.Способ постановки/снятия с охраны объекта и места расположения средств управления.
- 28.Время автономной работы сигнализации при отключении электроснабжения в дежурном режиме и режиме тревоги.
- 29.Требования эстетики и существующие возможности по прокладке проводов.

Примерный перечень вопросов для опросного листа по проектированию системы контроля и управления доступом

Общие вопросы

1. Количество зданий и входов в них, оснащённых системой СКУД.
2. Количество въездов на территорию объекта для транспорта.
3. Оснащены ли въезды инженерно-техническими средствами ограничения доступа (ворота, шлагбаумы и т.п)
4. Если на объекте есть зоны с разной степенью защищенности от проникновения, то укажите их количество и основные параметры.

5. Оценочная степень необходимой защищенности системы от проникновения методом копирования идентификаторов (низкая, средняя, высокая).

По оснащению турникетов средствами СКУД

6. Основной способ управления турникетами: проксимити-карты, биометрические считыватели, карты со штрих-кодом, считыватели touch-memory.
7. Если нужны картоприемники, то укажите их количество.
8. Если нужен дополнительный способ управления турникетами, то укажите его.

По оснащению шлагбаумов или ворот средствами СКУД

9. Длина стрелы шлагбаума.
10. Основной способ управления шлагбаумами: радиобрелки, кнопка у охранника, бесконтактные карты, активные метки на транспорте.
11. Интенсивность использования точки проезда (количество контролируемых транспортных средств в единицу времени).
12. Если нужны картоприемники, то укажите их количество.
13. Если нужен дополнительный способ управления шлагбаумом или воротами (управление от системы видеонаблюдения с автоматическим определением номеров), то укажите его.

Для оснащения дверей внутри здания средствами СКУД

14. Размеры и тип двери: металло-пластиковые, металлические, деревянные, стеклянные и т.п.
15. Основной способ управления замками СНАРУЖИ ДВЕРИ: проксимити-карты, биометрические считыватели, карты со штрих-кодом, считыватели touch-memory.
16. Способ управления замками ИЗНУТРИ ДВЕРИ: так же, как и снаружи, нажатием кнопки "выход".
17. Требования к эстетике монтажа запорных устройств (накладной монтаж, врезной монтаж).
18. Усилие удержания замками (150, 300, 500, 1000 и более кг).
19. Если дополнительно нужны картоприемники, то укажите их количество.
20. Если нужен дополнительный способ управления дверьми с замками, то укажите его.
21. Требования к дополнительной установке на дверь аудиодомофона или видеодомофона.
22. Необходимость установки доводчиков дверей.

Другие требования

23. Наличие проходных и бюро пропусков (выдача временных пропусков для прохода на объект).
24. Необходимость просмотра отчетов СКУД на ПК.
25. Количество компьютеров для просмотра отчетов СКУД по сети.
26. Количество сотрудников организации и количество возможных посетителей.
27. Необходимость учёта рабочего времени сотрудников.
28. Количество точек прохода, в которых должен фиксироваться приход/уход сотрудников.
29. Необходимость обнаружения фактов повторного прохода на объект без выхода с него, например, если один посетитель передал свой пропуск другому (функция antipassback).
30. Необходимость интеграции со службами администрирования компьютерных систем (например, Active Directory для управления удостоверениями и доступом).
31. Необходимость организации, количество и места расположения АРМ для отображения состояния и управления системой СКУД.
32. Возможность расширения системы в ближайшее время (появление новых объектов, увеличение количества сотрудников и т.п.).

В качестве альтернативы опросу, предложен вариант анкеты для получения первичной информации от заказчика при проектировании системы охранного видеонаблюдения. Анкета позволяет четко структурировать информацию для каждого элемента основного оборудования, входящего в состав подсистемы.

Примерное содержание анкеты для проектирования СОТ

Характеристики устройства записи/воспроизведения видеоинформации

1) Место установки устройств записи:

2) Тип устройства: ☐ регистратор ☐ компьютер с программно-аппаратным комплексом

3) Скорость записи, полей/сек/канал: ☐ 4 к/с ☐ 6 к/с ☐ 8 к/с
☐ 12 к/с ☐ 25 к/с ☐ 30 к/с ☐ 60 к/с

4) Количество подключаемых камер:

4) Количество дней хранения архива: ☐ 1 ☐ 3 ☐ 5 ☐ 7
☐ 14 ☐ 30 ☐ 45 ☐ 60

5) Другие требования к устройству записи:

- ☐ возможность просмотра по сети LAN/Internet
- ☐ возможность управления роботизированными камерами по сети LAN/Internet
- ☐ разграничение прав доступа к информации от камер или архиву
- ☐ наличие функций видеоанализа
- ☐ интеграция с СКД ☐ интеграция с ОПС
- ☐ интеграция с кассовыми терминалами
- ☐ наличие повышенной защиты данных архива средствами RAID

- 6) Нужна ли автономная работа при отключении электроэнергии: ☐ нет ☐ да,
а именно часов
- 7) Прочие требования:

Параметры устройств отображения видеoinформации

Монитор №....

1) Место расположения монитора:

2) Задача видеонаблюдения:

- 3) Тип монитора: ☐ компьютерный ☐ видеостена
- 4) Размер, дюймов: ☐ 15 ☐ 17 ☐ 19 ☐ 21 ☐ 24 ☐ более 24
- 5) Какие камеры надо просматривать: ☐ все ☐ выборочно, а именно:

- 6) Нужна ли автономная работа при отключении электроэнергии: ☐ нет ☐ да,
а именно часов
- 7) Прочие требования:

Параметры видеокамер:

Видеокамера №...

1) Место установки:

- 2) Цвет изображения: ☐ черно-белая ☐ цветная ☐ день/ночь
- 3) Передача изображения: ☐ аналоговый сигнал (HD) ☐ цифровой сигнал (Ethernet)
- 4) Тип исполнения: ☐ стандартный дизайн ☐ пальчиковая
☐ купольная простая ☐ купольная управляемая
☐ антивандальное исполнение
- 5) Условия работы камеры: ☐ внутри офиса ☐ на улице
☐ в неотапливаемом помещении
- 6) Что необходимо видеть: ☐ общее наблюдение ☐ действия персонала
☐ опознание своих людей ☐ опознание незнакомых
людей
☐ номера машин ☐ охрана периметра
- 7) Рабочая освещенность: ☐ офис/цех/склад днем ☐ искусственный свет
☐ дежурное освещение ☐ помещение без света
☐ освещенная улица ☐ неосвещенная улица
- 8) Изменение освещенности: ☐ постоянная ☐ переменная
- 9) Задняя подсветка объекта: ☐ есть ☐ нет
- 10) Расстояние до наблюдаемого объекта/участка:метров
- 11) Ширина наблюдаемого объекта/участка по фронту:метров
- 12) Условия монтажа: ☐ на стене ☐ к потолку
☐ на горизонтальную поверхность сверху
- 13) Материал поверхности: ☐ кирпич ☐ бетон ☐ дерево
☐ металл ☐ камень ☐
- керамика
- 14) Высота установка камеры относительно земли/пола:метров
- 16) Дополнительной вынос видеокамеры: ☐ по горизонтали ... см
☐ по вертикали см
- 17) Нужна ли автономная работа камеры при отключении электроэнергии:
☐ нет ☐ да, а именно..... часов

- 18) Общая длина кабеля от камеры до устройства записи: метров.
- 19) Другие требования к видеокамере: ☐ запись звука ☐ подключение динамика
☐ тревожный вход ☐ тревожный выход
☐ инфракрасная подсветка
☐ функции видеоанализа в камере

20) Прочие требования:

Условия монтажа проводов

Участок №...

1) Высота:

2) Материал:

- 3) Защита кабеля: ☐ короб ☐ металлорукав ☐ гофро-труба
- 4) Способ укладки: ☐ декоративно ☐ вдоль стен/потолков ☐ по воздуху
☐ за подвесным потолком
☐ по крыше ☐ вдоль трубы ☐ под землей

Полученная таким образом информация об объекте охраны и о требованиях к комплексу технических средств используется обучающимися для формирования концепции организации безопасности конкретного объекта от прогнозируемых угроз и ТЗ на проектирование интегрированной КСБ и ее функциональных подсистем.

5.2 Разработка концепции и технического задания на создание системы безопасности

Основным документом, который необходимо сформировать перед началом работ над ТЗ, является "Концепция безопасности объекта". В рамках учебного проектирования предлагается сформировать общую концепцию из расчета 2-3 страницы для каждой подсистемы. В этом документе должно быть обоснование необходимости формирования трех функциональных ПСБ (ОПС, СОТ и СКУД) для заданного объекта; определены цели и задачи, которые ставятся в структуре охраны объекта перед комплексом технических средств, его состав, роль и место, взаимодействие с другими системами жизнеобеспечения объекта. Излагается описание объектов защиты, потенциальных угроз, общие принципы организации и функционирования СБ, общие требования к функциональным ПСБ.

Современные ИСБ по своему составу и принципу работы стали ближе к автоматизированным системам. Поэтому для разработки ТЗ, которое определяет требования и порядок создания автоматизированной системы, уместно пользоваться ГОСТ 34.602-89 "Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы".

Графическими исходными данными для разработки концепции и ТЗ на создание интегрированной КСБ могут быть такие документы, как план территории объекта, архитектурно-строительные чертежи зданий и сооружений, план физической охраны объекта (в приложении к КП).

Состав и содержание ТЗ ИСБ также будут определяться требованиями конкретного объекта, необходимым составом ИСБ, этапностью развертывания ИСБ и другими факторами. Например, если заказчик определил, что объект будет оборудоваться по этапам, например: периметр, административное здание, производственная площадка, склады, то и в ТЗ есть смысл брать данные элементы за единицу разработки, включая все задействованные там подсистемы. Если объект оборудуется сразу, то за единицу разработки логично брать всю функциональную подсистему.

ТЗ призвано конкретизировать и дать числовое выражение требованиям заказчика к элементам систем безопасности, указанным в концепции – для осуществления объективного контроля их выполнения при сдаче системы в эксплуатацию. В рамках учебного проектирования следует брать за основу следующий состав ТЗ.

1. Наименование работы.

Здесь необходимо дать точное и полное наименование работы по созданию ИКСБ, указать название и адрес или местоположение учебного объекта.

2. Основание для создания ИСБ.

Как правило, это решение или документ заказчика, где определена необходимость оборудования объекта ИСБ, а также исходные данные: архитектурно-строительные чертежи, генплан объекта и т.п.

3. Цель и состав работы.

Целью работы является создание ИСБ объекта, соответствующей определенным техническим, технологическим, производственно-экономическим требованиям. Как правило, здесь же могут быть указаны критерии, по которым делается оценка достижения целей создания ИСБ. Так же можно отразить требования по стадийности и этапности создания ИСБ.

4. Исходные данные для проектирования.

От полноты и точности исходных данных во многом будет зависеть качество проектных работ.

- Описание объекта.

Описание объекта должно быть выполнено в такой форме и объеме, чтобы было ясно, на какую материально-техническую базу должна "наложиться" создаваемая ИСБ. В первую очередь это касается инженерных средств защиты (ограждений, заграждений, освещения, связи и т.п.), состояния и организации физической охраны (караулы, посты, маршруты движения и т.п.), а также других факторов,

влияющих на построение ИСБ. Необходимо дать краткую характеристику криминогенной и пожарной обстановки в месте расположения объекта, а также соседних объектов, граничащих с защищаемым объектом.

- Перечень основных регламентирующих документов, которыми должны руководствоваться заказчик, разработчик и исполнитель при выполнении работ по созданию ИСБ.

Общие требования к ИСБ.

В этом разделе объединены требования, единые для всех подсистем и системы в целом.

- Требования по назначению, составу и структуре
Здесь целесообразно дать определение ИКСБ как совокупности различных элементов и систем, работающих под единым управлением, а также указать, для выявления каких событий и действий она предназначена, какую информацию она должна формировать "на выходе".

Необходимо указать, из каких подсистем должна состоять ИСБ, алгоритм работы ИСБ, глубину интеграции подсистем, набор функций взаимодействия подсистем, интеллектуальные уровни, решающие задачи интеграции и управления компонентами, а также требования по защите самой ИСБ от преднамеренных и непреднамеренных действий по нарушению штатной работы системы.

Кроме того, важно указать, какими другими системами (например, лифтовое оборудование, освещение, вентиляция, пожаротушение, контроль технологических процессов, контроль процессов жизнеобеспечения) должна управлять или взаимодействовать проектируемая ИКСБ.

- Требования по размещению оборудования.

Требования по размещению основного и промежуточного оборудования, кабельным трассам достаточно полно изложены в нормативных документах.

Здесь необходимо конкретно указать место расположения центра управления ИКСБ, количество, состав и места размещения автоматизированных рабочих мест (АРМ). Если требуется изготовить специальные стойки, стеллажи, тумбы, столы, то необходимо сделать планы, чертежи в виде приложений или просто изложить требования к ним, оставив решение вопроса по дизайну за исполнителем.

- Требования по условиям эксплуатации

Здесь необходимо выдвинуть требования по климатическому исполнению оборудования, защите от электромагнитных помех,

агрессивной среды и т.п. Эти требования изложены в соответствующих ГОСТ.

- Требования к продолжительности непрерывной работы

При правильно организованном энергообеспечении система должна функционировать круглосуточно.

- Требования к электропитанию

Надо дать характеристику имеющейся электрической сети. Необходимо указать места подключения блоков ИСБ к существующей электрической сети. Если на объекте невозможно обеспечить электропитание ИСБ по первой категории, необходимо сформулировать требования по резервным источникам питания. Минимально необходимые требования по резервному электропитанию для различных подсистем ИСБ изложены в нормативных документах.

- Требования к возможности расширения и изменения конфигурации ИСБ

Если заказчик планирует расширение, изменение конфигурации ИСБ, то необходимо точно указать какие подсистемы, в каких размерах, в какие сроки будут этому подвержены. Проектная организация должна заложить соответствующий резерв возможностей ИСБ.

Требования к подсистемам ИСБ.

В этом разделе формулируются специальные требования к каждой функциональной ПСБ.

- Подсистема сбора и обработки информации (при программной интеграции подсистем)

В ИСБ данная подсистема, как правило, представляет собой программно-аппаратный комплекс. Поэтому надо сформулировать требования как к программной, так и к аппаратной части в виде функциональных и технических требований.

- Подсистема охранно-пожарной сигнализации

Наиболее важным элементом этой подсистемы являются извещатели. Для того чтобы проектная организация могла выбрать наиболее приемлемую модель извещателя, очень важно правильно и полно сформулировать признаки событий, которые должны классифицироваться извещателем, как "тревога", "саботаж" и "неисправность", а также возможные преднамеренные и непреднамеренные помехи в работе выбранных извещателей.

Важным требованием является тактика постановки и снятия с охраны разделов и зон, которую хотел бы реализовать заказчик. Кроме того, необходимо указать конкретные участки периметра, здания, сооружения, помещения, которые подлежат оборудованию охранной сигнализацией, и указать их особенности (например:

кассы, комнаты хранения оружия). Если планируется установка кнопок тревожной сигнализации или ловушек, требуется указать их вид и места установки. Необходимо также сформулировать требования к приемно-контрольным приборам, извещателям, оповещению о тревожных событиях, средствам передачи тревожных извещений (куда и в каком виде должен приходить сигнал).

- Подсистема контроля и управления доступом

Требования необходимо формулировать с учетом положений ГОСТ Р 51241-2008 "Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний". Необходимо указать требования к подсистеме по организации зон доступа, местам оборудования точек прохода и их пропускной способности, видам идентификационных признаков и устройствам идентификации, видам перекрытия проемов прохода, по штатной процедуре допуска персонала, посетителей и другие.

- Подсистема охранная телевизионная

Здесь необходимо указать, какие элементы объекта подлежат оборудованию данной подсистемой (периметр, контрольно-пропускной пункт, входы, коридоры, помещения, другие зоны прохода и места сосредоточения материальных ценностей). В качестве приложения должна быть представлена схема размещения видеокамер с обозначенными сценами и границами контроля. Для каждой сцены должны быть определены цели и задачи видеоконтроля. Отдельно должно быть оговорено применение поворотных видеокамер с трансфокаторами. Остальные требования к видеокамерам, устройствам обработки, записи и отображения, соединительным линиям, электропитанию можно сформулировать в соответствии с ГОСТ Р 51558-2014 "Системы охранные телевизионные. Общие технические требования и методы испытаний".

Требования к проектно-сметной, конструкторской, рабочей и эксплуатационно-технической документации (требования достаточно полно изложены в действующих нормативных документах).

5.3 Разработка проектных решений

5.3.1 Общие положения

При разработке проектных решений для каждой функциональной ПСБ в рамках ИКСБ следует придерживаться следующей последовательности действий и изложения материала.

1. Назначение подсистемы (на основе результатов предпроектного обследования и обоснования, данного в концепции).
2. Выбор и обоснование локальных зон контроля с привлечением

графической информации о плане, специфики функционирования и местоположении объекта.

3. Определение состава основного и вспомогательного оборудования, формирующего структурную схему подсистемы.
4. Выполнение расчетной части проекта для определения параметров основного оборудования, способного решить поставленные перед ПСБ задачи.
5. Выбор аппаратуры и программных средств для центрального пульта наблюдения и периферийных систем сбора, обработки информации и управления, оборудование АРМ, параметры серверов и жестких дисков для хранения информации.
6. Выбор средств обнаружения угроз, средств отображения информации, средств передачи тревожных извещений; описание их состава и характеристик.
7. Выбор вспомогательного оборудования и монтажных элементов.
8. Расчет параметров бесперебойного питания системы на основе требований к электрообеспечению (основное и резервное) и расчетов энергопотребления основных элементов подсистемы.
9. Разработка плана размещения оборудования в соответствии с представленным планом помещений и территорий объекта.
10. Разработка каналов связи для передачи информации.

Для программного обеспечения указывается производитель, операционная система, под которую оно разработано; количество каналов для подключения средств обнаружения угроз и для обеспечения удаленного доступа с помощью АРМ, поддерживаемые основные и дополнительные функции, ссылка на источник информации.

Для технических средств указывается полное название устройства, производитель, технические характеристики, особенности функционирования и эксплуатации, фото или рисунок, отражающие внешний вид, ссылка на источник информации.

При формировании кабельных магистралей для передачи информации указываются марки и параметры кабеля, входных и выходных разъемов, монтажного оборудования для подключения элементов проектируемых ПСБ и для их интеграции в рамках всех системы.

5.3.2 Порядок проектирования охранно-пожарной сигнализации

Выбор типа системы охраны

В зависимости от требований заказчика, топологии объекта, его архитектурных особенностей и географического расположения, могут использоваться проводные или радиоканальные сигнализации на основе цифровых и оптико-цифровых элементов.

Наиболее распространёнными являются проводные системы сигнализации.

Проводные системы с радиальной структурой (извещатели подключаются непосредственно к контрольной панели) обычно имеют не более 20-24 шлейфов, которые соотносят с зонами охраны. Дальнейшее увеличение количества шлейфов ведет к непропорциональному повышению стоимости монтажных работ и сложностям в эксплуатации системы [4, 6, 7].

Для построения сигнализаций более чем на 20 зон рекомендуется древовидная структура подключения извещателей: используют панели с дополнительными расширителями (концентраторами, модулями). Расширители подключаются к панели через специальную цифровую шину, длина которой может достигать 1000-1500 метров. Через шину к панели можно подключить различные адресные устройства: расширители шлейфов и выходов, клавиатуры, радиоприёмники, считыватели, панели индикации и другие элементы. Перечень моделей и количество подключаемых к шине ППК модулей указан в её описании и технической документации.

В беспроводных системах информация между извещателем и контрольной панелью передаётся по радиоканалу. В каждом извещателе кроме схем обнаружения вторжения в зону контроля имеется встроенный радиопередатчик и элемент автономного электропитания. Высокая стоимость радиоканальных систем по сравнению с проводными аналогами оправдана, когда:

- нет возможности проложить кабельное соединение;
- высока стоимость прокладки кабеля по обходному пути;
- восстановительный ремонт потребует больших затрат из-за дорогостоящей отделки помещений;
- невозможно использовать провода из-за уникальной отделки помещений (музеи, памятники).

Недостатками таких систем являются ограниченная дальность, подверженность помехам и отсутствие совместимости радиоканальных элементов разных производителей.

При выборе мест установки беспроводного оборудования необходимо учитывать влияние помех на радиосигнал. Для увеличения надёжности доставки сигналов и увеличения дальности в радиоканальных системах могут применяться ретрансляторы.

Возможно построение оптико-цифровых систем безопасности, сочетающих проводные и радиоканальные элементы. Такие комбинированные системы реализуются следующими конфигурациями:

- моноблочной (панелью со встроенным радиоприёмником и проводными шлейфами);

- модульной (проводной панелью с подключаемым к ней по проводам внешним радиоприёмником); при этом возможны два способа подключения внешнего приёмника к панели.
 - через цифровую шину, как правило, подключаются приёмник и проводная панель, выпущенная одним производителем;
 - через релейные выходы приёмника, которые срабатывают при поступлении сигнала от радиоканального извещателя; выходы приёмника подключаются в шлейф проводной панели; такой способ позволяет подключать приёмники радиосигнала от беспроводных извещателей к проводным панелям разных производителей.

Комбинированные системы применяются на объектах, где есть отдельные помещения или строения, существенно удаленные от основной части объекта или после дорогостоящего ремонта, не допускающего выполнение проводки.

Объекты защиты

Кроме защиты жизни сигнализации призваны защищать материальные ценности. Основными угрозами для имущества являются пожар, кража и грабёж.

Для каждого объекта, исходя из его особенностей, необходимо определить основные угрозы и источники возникновения пожара. Необходимо принять во внимание не только нахождение на объекте горючих предметов, но и материалы, из которых построено здание (дерево), отделочные материалы помещений (линолеум, панели ПВХ и т.п.). Особое внимание нужно уделить объектам, на которых есть:

- легко воспламеняющиеся, взрывчатые и химические вещества;
- промышленное оборудование, при работе которого выделяется большое количество тепла;
- мощные силовые электрические машины и механизмы;
- котлы, камины и печи отопления.

Определение возможных источников пожара помогает в дальнейшем правильно выбрать типы извещателей. Пожарные извещатели устанавливаются во всех помещениях, где возможно возгорание. Признаками появления возгорания являются задымление и быстрое повышение температуры в месте будущего очага. Поэтому наиболее распространены тепловые и оптико-электронные дымовые датчики.

Для выбора топологии и состава охранной сигнализации определяются материальные ценности, присутствующие на объекте, места и порядок их хранения и возможного перемещения. Деньги, ценные бумаги и драгоценности часто хранятся в сейфах или специально отведенных ящиках и шкафах. В коммерческих компаниях наличные денежные средства могут находиться в кассовых аппаратах. В торговых компаниях материальные ценности находятся не только на складе, но и на витринах в

торговой зоне. Предметы искусства сосредоточены в выставочных залах, галереях, музеях, частных коллекциях. Коммерческая информация и технологические секреты могут находиться на электронных носителях (компьютеры, ноутбуки, DVD диски, носители памяти и т.п.) и в бумажных документах. Территориально они могут находиться в кабинетах сотрудников компаний, имеющих доступ к ним. В качестве предметов защиты также следует рассматривать деньги и личные вещи сотрудников учреждения, находящиеся в служебных помещениях.

Определение целей вторжения на территорию объекта, модели наиболее вероятного нарушителя и наиболее вероятных сценариев его действий дает возможность сформировать требования к средствам системы охраны, при реализации которых возможно ее эффективное противостояние существующим угрозам.

При построении системы охраны необходимо защищать сами ценности, места их сосредоточения, а также подходы к ним. Извещатели размещаются на объекте, объединяются в группы по контролируемым зонам и образуют рубежи охраны.

Рубежи охраны

Эффективная структура сигнализации характеризуется необходимым количеством рубежей охраны, охраняемых зон, шлейфов в каждом рубеже и техническими возможностями её реализации на данном объекте.

Необходимая рубежность охраны материальных ценностей определяется в зависимости от их вида и концентрации в помещениях объекта. При этом следует учитывать ситуации, когда на объекте может быть несколько помещений, требующих многорубежной охраны.

Количество шлейфов сигнализации в каждом рубеже охраны определяется внутренней структурой объекта и протяжённостью его периметра. Для оперативного определения места срабатывания периметральных извещателей, рекомендуется в периметре выделять отдельные участки (фасад, тыл, левая сторона, правая сторона и т.п.) с контролем каждого участка самостоятельным шлейфом сигнализации. Самостоятельными шлейфами на объекте со сложной внутренней структурой могут быть выделены также отдельные зоны (переход, коридор и т.п.), организуемые на пути наиболее вероятного движения нарушителя к материальным ценностям или секретной информации. Самостоятельным шлейфом организуется на объекте тревожная сигнализация.

При оборудовании объектов охранно-пожарной сигнализацией с выходом на пульт централизованного наблюдения (ПЦН) необходимо также различать три следующие разновидности структуры построения каждого рубежа сигнализации:

- раздельную (пожарные и охранные шлейфы сигнализации подключаются к отдельным ППК с выходом каждого ППК на самостоятельный пультовый номер);

- отдельно-совмещённую (охранные и пожарные шлейфы сигнализации разделены и имеют свои ППК, но объединены на один пультовый номер);
- совмещённую (охранные и пожарные извещатели включены в один общий шлейф сигнализации или используются охранно-пожарные извещатели).

При централизованной тактике охраны рекомендуется отдельная структура шлейфов сигнализации как наиболее информативная и удобная в эксплуатации. При такой структуре пожарная сигнализация находится в дежурном режиме круглосуточно и контролируется ПЦН независимо от охранной сигнализации, которая в рабочее время отключается пользователем [6].

Количество рубежей охраны, физических барьеров, их взаимное расположение, физические принципы функционирования средств обнаружения в ряде случаев определяются ведомственными руководящими документами в зависимости от важности охраняемого объекта. Если объект не относится к категории важных, то данные вопросы определяются проектировщиком и установщиком системы ОПС.

Обычно используется от 2 до 7 рубежей охраны. Рубеж охраны часто «привязан» к естественным физическим барьерам или пространствам, которые преодолевает нарушитель на пути к ценностям при проникновении на объект. К таким барьерам относятся:

- граница объекта охраны (заборы, двери, живые изгороди и т.п.);
- открытая территория между границей объекта и зданиями;
- периметр зданий (стены, окна, двери, крыша);
- внутреннее пространство зданий (внутренние помещения, проходы, коридоры, лестницы);
- подходы к ценностям (подход к сейфу, входу на склад и т.п.);
- ценности или места их хранения (сейфы, картины, пачки денег в кассе и т.п.);
- места расположения основного оборудования сигнализации (ППК, СПИ и средств управления).

На преодоление физических барьеров рубежей охраны нарушитель тратит некоторое время. Чем раньше будет обнаружено вторжение на объект, тем меньше будет возможный ущерб (нарушитель может не успеть добраться до ценностей) и тем больше времени будет у сотрудников охраны для прибытия на объект.

Наиболее часто средствами охраны оборудуют: периметр здания, внутренние пространства помещений, подходы к ценностям и сами ценности.

Выбор извещателей и мест их размещения на объекте

Для выбора варианта установки оборудования на объекте необходимо представить, каким путём потенциальный преступник проник на объект.

Необходимо определить на уровне гипотезы возможные траектории движения нарушителя при проникновении на объект.

Рубежи необходимо оборудовать извещателями по принципу равной прочности со всех направлений – средства охраны должны образовывать замкнутый контур, чтобы нарушитель не смог беспрепятственно проникнуть на объект через незащищенный участок. Выбор типа каждого извещателя должен учитывать:

- специфику и способ преодоления рубежа охраны (воздействия на инженерно-технические укрепления, конструкции, ограждения);
- особенности обнаружения нарушителя извещателем на основе его физического принципа действия;
- наличие источников ложных срабатываний для него.

Необходимо выбрать извещатель и разместить его так, чтобы охраняемые предметы или пространство находились в пределах его зоны обнаружения.

Извещатели сигнализации основаны на разных физических принципах, направлены на обнаружение различных действий, имеют разные зоны обнаружения. Наиболее часто в системах охранной сигнализации используются:

- магнитоконтактный извещатель обнаруживает открытие разных конструкций: дверей, окон, ворот и т.п.;
- активный оптико-электронный (инфракрасный) извещатель обнаруживает движение по прерыванию инфракрасного луча между передатчиком и приёмником; зона обнаружения представляет собой узкую область длиной от 10 до 100 метров;
- пассивный оптико-электронный (инфракрасный) извещатель (ПИК) обнаруживает движение объектов, более тёплых или холодных относительно температуры окружающей среды; зона обнаружения определяется конфигурацией линзы Френеля, используемой в качестве оптической фокусирующей системы;
- микроволновый извещатель (МВ) реализует активный метод обнаружения движения объектов в зоне чувствительности каплевидной формы с высотой от 5 до 10 метров и телесным углом от 60 до 140 градусов при дальности действия поля от 10 до 15 м;
- комбинированные извещатели имеют два разных канала (как правило, ПИК+МВ), которые срабатывают на движение объекта;
- акустический извещатель обнаруживает появление звука разбивающегося стекла; зона конусообразной формы с высотой до 8 метров и телесным углом 120-160 градусов;
- емкостные извещатели обнаруживают приближение или прикосновение человека к крупным металлическим предметам или конструкциям (заборам, ограждениям, сейфам, металлическим дверям) по изменению емкости контролируемой поверхности;

- пьезоэлектрический извещатель обнаруживает механические вибрации (сверление или дробление) или ударные разрушающие воздействия на конструкции, на которые он установлен;
- температурный извещатель обнаруживает превышение заданного порога или необычно быстрый рост температуры в помещении;
- дымовой оптико-электронный извещатель реагирует на появление дыма, который рассеивает оптическое излучение (белый, серый, желтый дым).

Учитывая назначение и особенности работы перечисленных извещателей, а также выявленные способы преодоления рубежей охраны, выбирают типы извещателей по физическому принципу их работы в соответствии с представленной таблицей 2.

Таблица 2 – Рекомендации по выбору извещателей

	Магнито-контактный	Пассивный ИК	Активный ИК	Микро-волновый	ПИК + МВ	Акустический	Емкостной	Пьезо-электрический
Двери	+	+	+	-	-	+	5*	+
Окна	+	+	+	-	-	+	-	+
Стены	-	-	-	-	-	-	-	+
Помещения	-	+	-	+	+	-	-	-
Коридоры	-	+	+	+	-	-	-	-
Сейфы	+	-	+	-	-	-	+	+
Промышленные помещения	-	1*	3*	-	+	-	-	-
Помещения с животными	+	2*	+	-	-	4*	-	-

В таблице 2 знаком «плюс» обозначена возможность эффективного использования извещателя указанного типа для контроля состояния перечисленных в первом столбце предметов или помещений; знаком «минус» - отсутствие таковой возможности, в виду несоответствия физического принципа работы датчика способу внешнего воздействия на его чувствительный элемент. Цифрами перечислены случаи, когда при применении указанного извещателя надо обеспечить при выборе его модели наличие специфических функций, которые адаптируют извещатель для контроля состояния предмета или помещения:

1* Промышленные помещения + ПИК: использование моделей с высокой устойчивостью к э/м помехам, 4-х элементными сенсорами и иммунитетом от животных.

2* Помещения с животными + ПИК: использование моделей с высоким иммунитетом от животных или с диаграммой «штора» для блокировки оконных проемов.

3* Промышленные помещения + АИК: использование на больших дальностях действия и местах со сложной помеховой обстановкой.

4* Помещения с животными + Акустический извещатель: блокировка периметра помещения при помощи МК, пьезоэлектрических и акустических извещателей.

5* Двери + Емкостной извещатель: Блокировка внутренних двойных металлических дверей.

Ложные срабатывания являются одной из существенных проблем при эксплуатации системы сигнализации. Правильно спроектированная система должна иметь минимальный уровень ложных срабатываний. Для минимизации ложных тревог необходимо:

- правильно выбирать тип и параметры извещателя;
- монтировать извещатель, учитывая наличие и расположение источников ложных тревог и их характер;
- правильно устанавливать и настраивать параметры извещателя.

Каждый тип извещателей имеет свои причины возможных возникновений ложных срабатываний:

- магнитоконтактный извещатель может срабатывать при вибрации конструкций, на которые он установлен;
- активный оптико-электронный (инфракрасный) извещатель может срабатывать в сильный дождь, туман, при пересечении луча крупными животными, появлении высоких сугробов или при зарастании преграды травой или кустарником;
- пассивный оптико-электронный (инфракрасный) извещатель может срабатывать на движение крупных животных, прямого солнечного света, от ИК излучения сильно нагретых предметов и больших потоков тёплого (холодного) воздуха. Возможно срабатывание от электромагнитных помех, сильных вибраций поверхностей, на которые установлен извещатель;
- микроволновый извещатель может срабатывать от радиосигнала от электронного оборудования, передающегося на его рабочей частоте;
- комбинированные ПИК+МВ извещатели имеют высокую устойчивость к ложным тревогам, могут срабатывать на крупных животных, близких по размеру к небольшому человеку;
- акустический извещатель может сработать при появлении звука, похожего на звук разбивающегося оконного стекла (звон ключей);

- емкостные извещатели могут срабатывать при существенном изменении влажности или при появлении у ограды луж, кустарника или животных;
- пьезоэлектрические извещатели могут срабатывать на механические вибрации, не связанные с разрушением конструкции: строительство, крупный транспорт недалеко от защищаемой стены или двери;
- температурные извещатели практически не имеют ложных срабатываний, однако возможно его срабатывание при неправильном выборе места установки, например, рядом с термическим технологическим оборудованием или вблизи камина или в сауне;
- дымовые оптико-электронные могут работать не только на дым, но и при появлении дисперсных сред (частиц, взвешенных в газе): туман, пыль, аэрозоли.

Ложные срабатывания можно уменьшить правильным выбором типа и установкой извещателя с учетом их функциональных особенностей

Извещатели расставляются на объекте так, чтобы наиболее благоприятное для обнаружения датчиком направление движения нарушителя совпадало с вероятной траекторией (маршрутом) его движения при проникновении на объект.

Таким образом, учитывая свойства извещателей разных типов и вопросы снижения ложных срабатываний, необходимо выбрать места установки и параметры зон обнаружения извещателей на объекте.

Формирование шлейфов

В наиболее распространенных для небольших объектов неадресных ППК идентификация тревоги происходит с точностью до шлейфа, то есть контрольная панель не может различить срабатывание отдельных извещателей в шлейфе. Это может быть несущественно, например, если в одном шлейфе находятся однотипные извещатели, охраняющие одно помещение, выделенное в отдельную зону охраны, если нет необходимости различать его отдельные области.

На срабатывание шлейфов панель должна реагировать по-разному, например:

- пожарные извещатели должны активировать оповещатели, передачу извещения на ПЦН о пожарной тревоге, а, возможно, и включение системы пожаротушения;
- срабатывание магнитоконтактного извещателя на двери при входе на объект обычно включает временную задержку (таймер) включения тревоги, которая нужна для того, чтобы пользователь успел выключить систему ОПС;
- по срабатыванию тревожной кнопки панель отправляет тревожное извещение на ПЦН без включения внешних оповещателей.

В один шлейф включают только те извещатели, реакция панели на срабатывание которых, должна быть одинаковой.

Пожарные извещатели часто подключаются по 2-х проводной схеме с питанием по шлейфу. Охранные извещатели, как правило, подключаются по 4-х проводной резистивной схеме, где по одной паре проводов подаётся питание, а во второй паре проводов устанавливается оконечный резистор. При этом панель контролирует сопротивление шлейфа.

При эксплуатации ОПС пользователи могут активировать режимы частичной охраны, когда отдельные шлейфы снимаются с контроля. Например, на уровне рубежей охраны отключают внутренние рубежи (помещения в доме), но оставляют под охраной периметр здания и отдельные ценности (сейфы или кабинеты). Нежелательно включать в один шлейф извещатели от разных рубежей охраны.

Увеличение количества извещателей в одном шлейфе имеет предел, который определяется двумя причинами. Во-первых, следует учитывать указанные выше рациональные соображения по расстановке извещателей на объекте, особенностям программирования зон и случаев локализации неисправностей. Во-вторых, есть технические ограничения, связанные с контролем со стороны панели сопротивления охранного или тока пожарного шлейфа. Увеличение количества извещателей приводит к увеличению длины кабеля, появлению в электрической цепи шлейфа дополнительных сопротивлений на внутренних элементах извещателей (реле). Техническое ограничение может быть рассчитано из условия сохранения суммарного сопротивления охранного шлейфа ниже установленного в документации предельного значения для конкретной панели в режиме "Норма". Для пожарных шлейфов увеличение количества извещателей приводит к росту суммарного тока в шлейфе, который не должен превысить заданной в документации на ППК токовой нагрузки в двухпроводном пожарном шлейфе.

Учитывая распределение извещателей по рубежам охраны, реакцию панели на их срабатывание, необходимость отключения шлейфа с охраны или по причине неисправности, необходимо выполнить распределение извещателей по шлейфам. В результате определяются требования к панели по количеству шлейфов.

Независимые разделы охраны

На объекте охраны часто существуют области, постановку и снятие с охраны которых необходимо производить независимо друг от друга. Типичными являются следующие случаи:

- несколько юридических лиц располагаются в одном здании;
- в одном здании находятся разные подразделения одной компании, имеющие разный режим работы;
- за помещения несут ответственность разные люди;
- при рассмотрении частных владений могут быть помещения и территории разного назначения: разные этажи жилой зоны, гараж, баня, подвал, помещения с оборудованием и коммуникациями.

В таких случаях возможно применение в системе нескольких ППК, по одному для каждого обособленного элемента объекта. Более удобным и экономичным является использование панелей большой ёмкости с функцией разделения на независимые разделы (области, подсистемы).

Деление системы на независимые разделы производится на уровне шлейфов, поэтому все извещатели в одном шлейфе будут отнесены к тому разделу, к которому «приписан» данный шлейф.

Таким образом, с учетом распределения извещателей по рубежам охраны, понимания режимов работы объекта, разделения объекта на независимые разделы, уточняются требования для выбора ППК.

При этом необходимо обеспечить возможность масштабирования системы в дальнейшем.

Управление системой ОПС

Способ управления системой должен быть оговорен в ТЗ. Основной операцией управления системой ОПС является постановка/снятие объекта с охраны, которая возможна следующими средствами:

- на объекте охраны с использованием проводных устройств (кнопок панели управления, клавиатур, контактных считывателей);
- дистанционно, с использованием радиобрелков или различных вариантов подключения по каналу GSM (SMS или приложений на основе GPRS/3G);

Для проводных устройств управления нужно определить их количество и места установки. Для этого необходимо определить порядок входа и выхода на территорию объекта или независимых разделов охраны пользователями системы. Устройства управления размещаются внутри объекта, рядом с привычными для пользователя входами в помещение. Подходы к устройствам управления должны быть защищены извещателями и контролироваться системой охраны.

В случае дистанционного управления системой ОПС сигналы передаются по радиоканалу. Для радиобрелков нужно учитывать ограниченную дальность передачи сигнала и размещать приёмные устройства ближе к местам входа на объект. Количество брелков управления в системе определяется количеством пользователей.

Таким образом, выбираемая контрольная панель должна поддерживать необходимое количество брелков управления или иметь соответствующее количество кодов пользователей для управления сигнализацией с помощью клавиатуры.

На плане объекта необходимо обозначить места размещения устройств управления.

Программируемые выходы (PGM)

Для решения задач управления внешними устройствами, а также для интеграции ОПС с системами видеонаблюдения, пожаротушения, голосового оповещения, СКУД контрольная панель должна передавать

электрические сигналы. Для этого используются программируемые выходы (*PGM*), которые являются опцией для контрольных панелей. Они могут располагаться как на плате самой панели, так и на специальных модулях расширения и могут быть двух типов:

- релейные, коммутируют достаточно большие токи до 3-5 А;
- транзисторные (могут иметь название в описании ППК «открытый коллектор»), переключают токи до 0,1 до 0,3А.

В случае подключения к программируемому выходу панели внешнего устройства, с током потребления больше, чем ток коммутации, выход выйдет из строя.

PGM может использоваться для передачи сигналов на СПИ о различных событиях в системе (например, тревога охранная, тревога пожарная), для включения или выключения режима охраны, отключения питания 220В и переключении на резервное питание. В этом случае для каждого передаваемого события нужен отдельный выход *PGM*. Важной функцией панели с использованием *PGM*-выходов также является управление средствами оповещения на объекте охраны.

При выборе контрольной панели необходимо учитывать требуемое количество *PGM* и их тип (транзисторный или релейный).

Оповещатели

Информация о способе, содержании и направленности оповещения на объекте для достижения максимальной эффективности извлекается из результатов предпроектного обследования.

Для привлечения внимания людей используются световые, звуковые и комбинированные оповещатели. Звуковые (сирены, громкоговорители) и световые (строб-вспышки, световые табло, проблесковые маячки) оповещатели размещаются по территории объекта охраны в помещениях и на открытом воздухе. Одна сирена может охватывать сразу несколько помещений, однако громкость звучания существенно снижается на больших расстояниях и при прохождении сигнала через стены. Световые оповещатели эффективны на больших открытых пространствах – больших помещениях, прямых коридорах или на улице.

Оповещатели эксплуатируются в отапливаемых и неотапливаемых помещениях, на улице, поэтому параметры температуры эксплуатации и класс пылевлагозащищенности (*IP*) оборудования должны быть соответствующими.

На объектах, где возможно механическое повреждение оборудования из-за неосторожности, вандализма, целесообразно выбирать оповещатели в вандалозащищённых корпусах. Желательно выбирать модели оборудования с одинаковыми номиналами по напряжению питания, что упростит дальнейший расчет и выбор блоков питания.

Система передачи извещений

Большинство систем сигнализации передают информацию (извещения) о своём состоянии на пункт охраны и могут получать управляющие сигналы. Информативность СПИ (количество видов передаваемых извещений) должна быть оговорена в ТЗ на проект. В ходе предпроектного обследования объекта формируются данные о возможных каналах связи для передачи тревожных извещений.

Изучив достоинства и недостатки СПИ на основе имеющихся на объекте проводных и беспроводных каналов связи, необходимо выбрать и аргументированно предложить один из типов СПИ, обладающей информативностью не ниже заданной.

Многие контрольные панели имеют элементы СПИ либо интегрированные на основную плату, либо в виде отдельных модулей, которые покупают и подключают при необходимости.

В рамках проекта СПИ выбирается с учетом существующих каналов связи с удаленными объектами, требуемой информативности и способа подключения к ППК.

Выбор контрольной панели

Таким образом, в результате предпроектного обследования объекта и анализа требований технического задания, можно выбрать ППК по совокупности выявленных параметров:

- тип системы (проводная, радиоканальная, комбинированная);
- количество рубежей, зон и шлейфов;
- количество независимых разделов;
- количество программируемых выходов (*PGM*) и их тип;
- количество устройств управления и кодов пользователей;
- информативность и проколы передачи данных для встроенных СПИ.

Выбранный ППК по своей архитектуре и параметрам должен обеспечивать возможность создания системы с протяженностью линий связи, шлейфов, дальностью радиоканальных систем, которые соответствуют размерам и особенностям территориального распределения объекта охраны. При выборе радиоканальных систем необходимо учитывать ряд ограничений:

- по дальности передачи радиосигнала;
- по необходимому количеству радиоканальных зон охраны;
- по наличию у выбранного производителя необходимого ассортимента извещателей и элементов управления (клавиатур, брелоков).

Подбираются элементы расширения для ППК: концентраторы для обеспечения необходимого количества шлейфов, платы программируемых выходов, модули бесконтактных считывателей, радиоприёмников и т.п.

Выбираются оповещатели по требуемым типам сигнала оповещения, (звуковой, световой или комбинированный), условиям эксплуатации, электрическим параметрам подключения к ППК.

В рамках курсового проектирования предлагается воспользоваться рекомендациями, сформулированными на основе обобщенной методики оптимизации выбора ППК для охраны объекта, которая соответствует нормативным документам, принятым во вневедомственной охране МВД России [8, 10].

Электроснабжение и монтаж элементов системы

На данном этапе проектирования выбираются источники бесперебойного питания, которые осуществляют электроснабжение сигнализации в нормальном режиме от внешних сетевых источников через трансформаторы и платы бесперебойного питания. В аварийном режиме, при отсутствии напряжения от внешнего источника, электроснабжение осуществляется за счет энергии аккумуляторных батарей, которые также необходимо выбрать на основе расчетов.

Время работы источников бесперебойного питания (ИБП) в автономном режиме должно обеспечивать надежное питание потребителей в течение времени, определяемого нормативами или достаточного для надежного закрытия функционирования систем безопасности с гарантированным сохранением целостности всех событий и баз данных (определяется техническими характеристиками оборудования и оговаривается в задании на проектирование).

Номинальные напряжения резервных источников питания постоянного тока должны выбираться из ряда: 12В, 24В.

Необходимо определить номенклатуру напряжений питания и токов потребления в выбранном оборудовании ОПС. Сгруппировать потребителей с одинаковыми напряжениями питания. Далее при выборе аккумулятора и ИБП следует выполнить следующие действия [9].

1. Составить список используемого оборудования (потребителей), разделив его на три категории:

- приборы, которые включены всегда, и не имеют своего штатного сетевого источника питания (датчики, камеры и т.п.) – обозначим для них ток потребления I_1 ;
- приборы, которые включены всегда, но имеют свой штатный источник питания (обычно это ППК, мониторы и т.п.) – обозначим для них ток потребления I_2 ;
- приборы, которые будут включаться периодически и кратковременно (сирены, узлы пожаротушения и т.п.) – обозначим для них ток потребления I_3 .

2. Просуммировать ток потребления приборов для каждой из трех категорий.

Очевидно, что ток, который должен обеспечивать источник при наличии сети $I_c = I_1$. Ток, который должен обеспечивать источник при отключении сети от резервных батарей $I_p = I_1 + I_2$. Ток, который должен обеспечивать источник кратковременно (в зависимости от времени работы устройств третьей категории) $I_k = I_1 + I_2 + I_3$.

Если ток I_c превосходит 2А, необходимо проанализировать, существует ли возможность разделить питание аппаратуры по группам.

Применение нескольких ИБП предпочтительно с точки зрения монтажа, особенно на объектах, имеющих большую протяженность (нельзя забывать о потерях на соединительных проводах), и существенно повышает надежность всей системы в целом. Разница в цене нескольких маломощных источников и одного мощного обычно незначительна.

Разделение нагрузки на несколько источников также целесообразно при необходимости обеспечить длительное время резервирования. Связано это с тем, что подавляющее количество источников рассчитано на работу с АКБ емкостью 7 или 11 Ач, а это означает, что ток 2А в течении 6 часов уже получить не удастся. В таком случае стоит разбить нагрузку на два источника с током 1А каждый и емкостью 7 Ач. Стоимость обеспечения питания при этом вырастет несущественно.

При разделении нагрузки на несколько групп указанные выше токи следует определить для каждой группы.

3. Задать необходимое время резервирования t , выраженное в часах.

Применительно к системам охранной, тревожной и пожарной сигнализации автономная работа оборудования должна обеспечиваться в течение не менее 24 ч в дежурном режиме и не менее 3 ч в режиме тревоги. (НПБ 88-2001*, РД 78.36.003-2002). Тогда требуемую емкость АКБ для обычных источников без преобразования напряжения батареи можно рассчитать по формуле:

$$A_T = 1,3 \cdot I_p \cdot t.$$

Коэффициент 1,3 следует применять, поскольку в нормальных условиях эксплуатации аккумулятор способен отдавать не более 70 % емкости.

В случае использования ИБП с преобразованием напряжения АКБ (АКБ имеют напряжение 12В, поэтому выходное напряжение в 24В получают за счёт преобразования), необходимо полученную емкость умножить на коэффициент преобразования и увеличить на 30 %, чтобы компенсировать потери при преобразовании.

Например, если используется ИБП с одним аккумулятором 12В, а на выходе схема должна дать 0,8А при напряжении 24В (то есть коэффициент

преобразования равен двум), то для обеспечения 4 часов бесперебойной работы нужно иметь емкость АКБ: $A_T = 1,3 \cdot 0,8 \cdot 4 \cdot 2 \cdot 1,3 = 10,8 \text{ [Ач]}$.

В случаях установки блоков бесперебойного питания в неотапливаемых помещениях необходимо учитывать зависимость емкости АКБ от температуры [10]. Определить фактическую емкость АКБ можно по формуле: $A_{\phi} = A_T \cdot K_t$, в которой значение коэффициента пересчета K_t можно определить из представленной ниже таблицы 3.

Таблица 3 – Для выбора коэффициента пересчета при определении емкости АКБ с учетом температуры эксплуатации

Коэффициент пересчета	Температура, °C								
	-40	-30	-20	-10	0	10	20	30	40
K_t	0,37	0,55	0,65	0,75	0,84	0,92	1,0	1,08	1,09

АКБ малых ёмкостей имеют нелинейную зависимость тока нагрузки и времени работы. Для выбора емкости АКБ удобно использовать таблицу значений (таблица 4), полученных с помощью инструментов проектирования ИБП на сайте производителя [10].

Таблица 4 – Для предварительного выбора емкости АКБ по требуемому времени работы в автономном режиме

Емкость АКБ, Ач	Время работы АКБ, ч							
	1	1,5	2	3	4	5	7	10
	Ток нагрузки, А							
1,2	0,6	0,4	0,3	0,2	-	-	-	-
4,5	3,5	1,7	1,2	0,8	0,5	0,4	0,3	0,2
7,0	6	3,5	2,5	1,5	1	0,8	0,5	0,3
12	11	7	5	3,5	2,5	1,8	1	0,6
18	17	11	8,0	5	3,5	2,5	1,5	1
26	26	16	12	8	5,5	4	3	2
40	40	27	20	13	9,5	7	5	3

Пропуски в таблице объясняются наличием предельно возможных токов, которые может обеспечить АКБ различной ёмкости.

4. Выбрать модель ИБП на сайте производителя на основе расчета токов I_c , I_p , I_k и емкости АКБ.

В самом простом случае, а также если не удастся разделить нагрузку по типам потребителей, выбирается ИБП, который сможет обеспечить I_k — самый большой из токов. При выборе блока питания необходимо использовать значение **номинального тока**, который может выдавать ИБП длительный период времени. Будет ошибкой ориентироваться на значение **максимального тока**, указанного в технической документации на ИБП, так

как блоки питания рассчитаны для работы в таком режиме всего несколько секунд или минут, после чего могут выйти из строя.

Таким образом, количество и мощность ИБП выбирается в зависимости от общего энергопотребления оборудования систем безопасности и необходимого времени работы в автономном режиме.

5. Сделать расчёт параметров АКБ согласно указанным временным промежуткам. Произвести окончательный выбор системы питания: моделей и количества единиц оборудования всех её элементов. Добавить соответствующую информацию в спецификацию оборудования.

Выполнить ориентировочную расстановку всех элементов системы безопасности на плане объекта охраны. ИБП следует размещать в помещениях охраны, пультовых, аппаратных или местах, не доступных для посторонних лиц и удобных для обслуживания.

Указать все кабельные соединения между элементами и обозначить количество проводов в каждом кабеле и их сечение. Сгруппировать провода по типам, количеству проводников, сечению и выбрать номенклатуру требуемой кабельной продукции. По плану объекта определить длину всех линий и подсчитать суммарные потребности проводов всех типов.

Участки коммуникаций на улице или в помещении могут требовать монтажа с применением гофрированных труб, кабельных коробов или металлорукава. Определить суммарные потребности в данных материалах. Необходимо учитывать, что в одном коробе или гофрированной трубе можно проложить несколько проводов одновременно.

Сформировать спецификацию выбранного оборудования и кабельной продукции с указанием их моделей, количества и их основных параметров. Зафиксировать расстановку элементов и коммуникации между ними на плане объекта охраны.

Скорректировать сформированную структурную схему (схемы) функциональной ПСБ, которая отражает взаимодействие основных элементов охранной, пожарной и тревожной сигнализаций.

5.3.3 Порядок проектирования системы охранного телевидения

Выбор типа видеосистемы

Автоматизированная СОТ на базе оптико-цифровых систем позволяет решать различные задачи на объекте охраны: выявление и видеофиксацию несанкционированного проникновения на территорию и в помещения, контроль поведения людей на объекте и прилегающих территориях, мониторинг движения транспортных средств, документирование видеoinформации о внештатных и тревожных ситуациях и другие.

Основным назначением СОТ при интеграции с охранными системами является видеоверификация тревожного события, зафиксированного извещателем, или выявление факта ложного срабатывания извещателя с

обязательным документированием видеоинформации, формированием архива записи для последующего анализа состояния объекта.

Предварительный выбор стандарта оборудования видеонаблюдения (аналогового, *IP*, *HD-TVI*, *HD-CVI* и *AHD*) производится экспертным методом на основе анализа ряда факторов.

IP-системы предпочтительны на крупных территориально распределенных объектах с большим количеством камер, удаленных постов наблюдения, с высокими требованиями к разрешению изображения, к наличию функций видеоанализа и многих других факторов. Однако, указанные системы относительно дороги, требуют от монтажника и проектировщика знаний и навыков в области *IT*-технологий.

Системы на базе аналоговых камер используются на локальных объектах, в условиях ограниченного бюджета, при малом или среднем количестве ВК, минимальных требованиях по видеоанализу изображения или записи архивов большой длительности.

В отдельных случаях возможно одновременное применение систем разных технологий видеонаблюдения. Рекомендуется использовать информацию из таблицы 5 для обоснования выбора технологии системы видеонаблюдения.

Таблица 5 – Сравнение параметров актуальных цифровых и аналоговых технологий видеонаблюдения

Технология	Аналог CVBS	HD-TVI (4.0) *	HD-CVI (3.0) *	AHD (3.0) *	IP
Тип сигнала	Аналоговый	Аналоговый	Аналоговый	Аналоговый	Цифровой
Разрешение (МП)	0,4 (960Н)	4	4	3	До 50 и выше
Совместимость оборудования разных производителей	Да	Да	Нет	Да	Ограничена (ONVIF, PSIA)
Возможности видеоанализа	минимальны	минимальны	минимальны	минимальны	максимальны
Передача по коаксиальному кабелю	До 200м	До 500м	До 1200м	До 500м	Устаревшее решение
Приёмопередатчик и по витой паре 3 категории	Да (до 2км)	Да	Да	Да	Нет
Витая пара 5 категории (UTP) по Ethernet	Нет	Нет	Нет	Нет	100хN**
Оптоволокно по Ethernet (1 отрезок между коммутаторами)	Нет	Нет	Нет	Нет	до 2000 м (для 1000BASE-F X) до 5000 м

Технология	Аналог CVBS	<i>HD-TVI</i> (4.0) *	<i>HD-CVI</i> (3.0) *	<i>AHD</i> (3.0) *	<i>IP</i>
					(для 1000BASE-L X)
Стоимость решения	Низкая	Низкая	Средняя	Низкая	Высокая

* - номер актуальных версий технологий композитного видеоинтерфейса высокой четкости, представленных мировыми производителями программных продуктов для аналогового видео:

HD-TVI (4.0) (*High Definition Transport Video Interface*) – открытая технология; разработчик и владелец компания *Techpoint Inc.*, Калифорния, реализуется в оборудовании под торговой маркой **Hikvision**, из отечественных — *RVI*, *Space Tehnology*, *LTV* и другие. (<http://www.techpointinc.net/products.html>);

HDCVI (3.0) (*High Definition Composite Video Interface*) – закрытая технология, разработчик и владелец компания *Dahua Technology HANGZHOU, CHINA*, оборудование не может быть изготовлено другим производителем без лицензирования у *Dahua*. (http://www.dahuasecurity.com/products_category/hdcvi-camera-388.html);

AHD (3.0) (*Analog High Definition*) – открытая технология, разработчик и владелец компания *Nextchip, Korea*; отличается прекрасной реализацией мультигибридности, когда даже самые недорогие видеорегистраторы способны работать сразу с тремя видами видеокамер – стандартными аналоговыми, *AHD*, *IP* (http://www.nextchip.com/eng/products/ahd_main.asp).

**- количество коммутаторов на линии соединения.

Последующий выбор моделей ВК и устройств записи видеoinформации производится из ассортимента выбранного типа видеосистемы.

Выбор и обоснование зон видеоконтроля

Характеристика объекта охраны и целевые задачи видеосистемы формируют подход к её созданию путем рационального выбора зон видеоконтроля и обеспечения необходимого качества видеоизображения на всех этапах его востребованности.

Проектирование видеосистемы проводится с учетом выполнения следующих требований:

- обеспечение качества изображения, соответствующего определенной задаче видеоконтроля в каждой зоне (обнаружения, различения или идентификации объекта контроля);
- обеспечение различных параметров изображения по разрешению и скорости записи и отображения видеoinформации для разных зон контроля и состояния детектора движения;

- обеспечение необходимого времени хранения видеoinформации и защищенного структурированного доступа к архиву и к функциям настройки системы со стороны пользователей.

Исходя из указанного подхода к созданию системы, с учетом результатов предпроектного обследования, необходимо в первую очередь выделить на рабочем плане объекта зоны видеоконтроля (критические зоны) и определить для них в пояснительной записке целевые задачи.

Таким образом, определяется приблизительное количество видеокамер (ВК) в системе, места их расположения и оборудование, необходимое для их оснащения и передачи видеосигнала.

Видеокамеры

Для сформированных зон видеоконтроля на объекте конкретизируют выбор мест установки камер и направления из обзора. При этом нужно учитывать ракурс наблюдения для выполнения задачи (например, невозможно определить номер машины или лицо человека при обзоре сверху). При расстановке камер учитывается существование неблагоприятных факторов для видеосъемки: "мёртвых" зон у камер, наличие и расположение источников освещения, источников ярких засветок (солнца, прожекторов, встречных камер с ИК подсветкой), объектов, создающих тень в течение времени наблюдения и т.д. Если неблагоприятные факторы невозможно избежать рациональной расстановкой камер, необходимо их компенсировать за счёт наиболее популярных функций видеокамер:

- Wide Dynamic Range (WDR) – функция широкого динамического диапазона, позволяет просматривать одновременно и сильно засвеченные участки, и области с малым уровнем освещенности на одном изображении;
- Digital Wide Dynamic Range (D-WDR) – цифровое расширение динамического диапазона за счёт обработки изображения процессором (DSP) видеокамеры;
- High Light Compensation (HLC) или Highlight Suppression Back LC (HSBLC) – функция компенсации засветки, маскирует яркие участки, заменяя их тёмной маской, при этом средняя яркость кадра значительно снижается, и затемненные участки изображения становятся видны.

Параметры и функции ВК, как правило, указываются в технической документации на сайтах производителей или дилеров видеооборудования.

Для наблюдения за большими открытыми площадками с высокими требованиями к разрешению изображения применяют поворотные (PTZ) видеокамеры. В этом случае от одной до трех широкоугольных стационарных камер обеспечивают обзор (и запись) общей обстановки, а поворотная камера используется для детального наблюдения оператором

критического события. Недостатками являются обязательное наличие на объекте оператора наблюдения и невозможность наблюдения одной поворотной камерой нескольких критических событий, происходящих в разных направлениях наблюдения одновременно.

После выбора типов и мест размещения видеокамер выполняется расчёт и выбор разрешения матрицы, фокусного расстояния объектива, требуемых углов обзора в соответствии с целевой задачей видеоконтроля.

Расчёт разрешения для разных задач видеонаблюдения возможно проводить по параметру плотности пикселей на 1 метр наблюдаемой площадки [1]. Значение параметра плотности пикселей в зависимости от задачи приведены в таблице 6.

Таблица 6 – Критерии для выбора матрицы видеокамеры по параметру плотности пикселей

Задача наблюдения	Плотность пикселей на 1 метр
Обнаружение человека*	30
Обзор (определение примет)*	60
Распознавание лица*	125
Идентификация лица*	250
Чтение автомобильного номера**	330
Идентификация игровой карты	550
Идентификация банкноты	365

* по стандарту IEC 62676-4 (международный стандарт - Международная электротехническая комиссия (МЭК), англ. International Electrotechnical Commission)

** по стандарту AS-4806.2 (Австралийский стандарт)

Для заданной ширины зоны наблюдения и в зависимости от целевой задачи рассчитывается требуемое горизонтальное разрешение для видеокамеры.

В настоящее время используются видеокамеры с разным форматом матрицы и с разными пропорциями размеров чувствительной площадки. Формат матрицы существенно влияет на углы обзора видеокамеры, а, следовательно, и на размеры области интереса и дистанцию, на которой возможно решение целевой задачи видеонаблюдения. В таблице 7 приведены данные о максимальной дистанции до объекта для камер с матрицами разных форматов. Расчёт сделан для камер с разрешением 2Мп (1920×1080) и соотношением сторон 16:9 для объектива с фокусным расстоянием 3,6мм.

Расчет фокусного расстояния и углов обзора объективов видеокамер выполняется по следующим формулам:

$$f_{\text{в}} = a \cdot D/V; \quad f_{\text{г}} = b \cdot D/H,$$

$$\alpha_{\text{в}} = 2 \cdot \arctg\left(\frac{V}{D}\right), \quad \alpha_{\text{г}} = 2 \cdot \arctg\left(\frac{H}{D}\right),$$

где $f_{\text{в}}$ и $f_{\text{г}}$ – фокусные расстояния объектива для охвата поля зрения по вертикали и горизонтали, соответственно, мм; $\alpha_{\text{в}}, \alpha_{\text{г}}$ – углы обзора объектива по вертикали и горизонтали, соответственно; a – высота матрицы, мм; b – ширина матрицы, мм; D – максимальное расстояние до объекта, м; V – высота объекта, м; H – ширина объекта, м.

Таблица 7 – Результаты расчёта максимального расстояния от камеры до объекта для разных целевых задач

Задача видеоконтроля	Максимальное расстояние от камеры до объекта, м							
	1"	2/3"	1/2"	1/2,5"	1/2,7"	1/2,8"	1/3"	1/4"
Обнаружение (30)	15,6	23,4	31,2	39,0	42,1	43,7	46,8	62,4
Распознавание (125)	3,8	5,6	7,5	9,4	10,1	10,5	11,2	15,0
Идентификация (250)	1,9	2,8	3,8	4,7	5,1	5,3	5,6	7,5
Чтение номера автомашины (330)	1,4	2,1	2,8	3,6	3,8	4,0	4,3	5,7

Геометрические параметры матрицы для расчета можно взять в таблице 8 с учётом формата матрицы и соотношения ее сторон.

Таблица 8 – Размеры матриц разного формата и соотношения сторон

Формат матрицы	Ширина, мм	Высота, мм	Диагональ, мм	Формат матрицы	Ширина, мм	Высота, мм	Диагональ, мм
Соотношение сторон матрицы 4:3				Соотношение сторон матрицы 16:9			
1"	13,54	10,16	16,93	1"	14,76	8,30	16,93
2/3"	9,04	6,78	11,28	2/3"	9,84	5,54	11,28
1/2"	6,77	5,08	8,47	1/2"	7,38	4,15	8,47
1/2,5"	5,42	4,06	6,77	1/2,5"	5,90	3,32	6,77
1/2,7"	5,02	3,76	6,27	1/2,7"	5,47	3,07	6,27
1/2,8"	4,84	3,63	6,05	1/2,8"	5,27	2,96	6,05
1/3"	4,52	3,39	5,64	1/3"	4,92	2,77	5,64
1/4"	3,39	2,54	4,23	1/4"	3,69	2,08	4,23

Из рассчитанных значений фокусных расстояний выбирают меньшее для охвата всего поля зрения. Затем выбирают объектив с равным или ближайшим меньшим фокусным расстоянием (в соответствии с ассортиментом выпускаемых объективов).

Далее определяются «мёртвые» или «слепые» зоны обзора. Это часть зоны видеоконтроля, которая не просматривается видеокамерой. Зона, контролируемая одной ВК, ограничена углом поля зрения α и максимальной дальностью наблюдения L_M . (рис. 1). Кроме того, в непосредственной близости от ВК качество изображения может ухудшиться вследствие ограниченной глубины резкости.

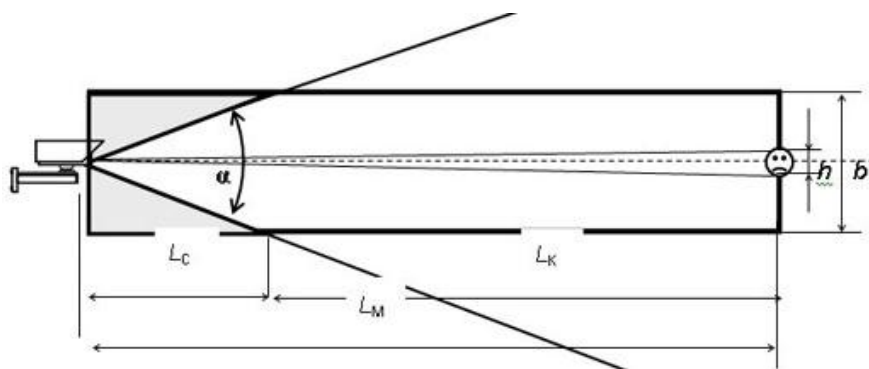


Рисунок 1 – Для определения «слепых» зон обзора

Протяжённость "слепого" участка L_C (ближняя граница контролируемого участка) определяется размером зоны b , фокусным расстоянием объектива f и размером матрицы d :

$$L_C = bf / d .$$

Максимальная дальность **обнаружения** человека определяется, исходя из критерия достаточности чёткости [11] – не менее 10% раstra на высоту человека h . Будем считать, что это обеспечивает классификацию тревожной ситуации оператором СОТ. В данном случае телевизионная дальность обнаружения выражается формулой:

$$L_M = 10 \frac{hf}{d} .$$

В результате размер контролируемой зоны определяется из следующего соотношения:

$$L_K = L_M - L_C = \frac{f}{d} (10h - b) .$$

Очевидно, что для увеличения размера L_K контролируемой зоны имеется единственный способ – увеличивать фокусное расстояние объектива. Вместе с тем, увеличивать фокусное расстояние чрезмерно нельзя, так как при этом возрастает размер "слепой" зоны.

Как правило, ВК устанавливаются на некоторой высоте H над поверхностью участка, за которым ведётся наблюдение. В результате такого расположения геометрические соотношения в вертикальной плоскости принимают вид, представленный на рис. 2.

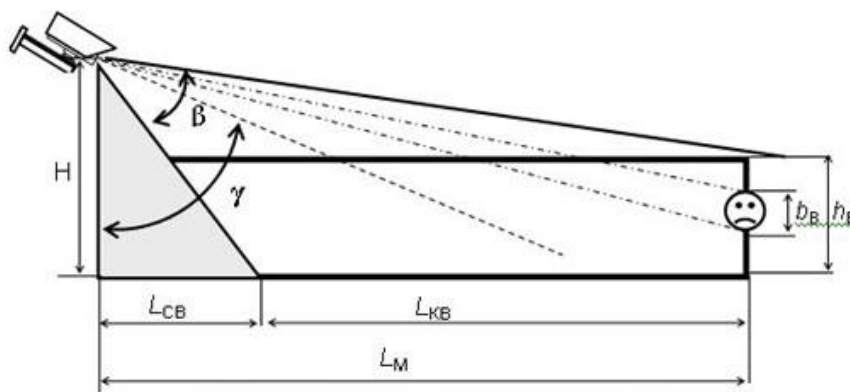


Рисунок 2 – Вертикальное поле зрения видеокамеры

Размер "слепой" зоны L_{CB} в вертикальной плоскости зависит от выбранного угла наклона ВК (угла γ между осью визирования и вертикалью) и угла зрения β камеры в вертикальной плоскости (в соответствии с принятым стандартом разложения составляет 3/4 от угла зрения телекамеры по горизонтали):

$$L_{CB} = L + H * \operatorname{tg}(\gamma - \beta / 2),$$

где L – расстояние от стены, на которой установлена ВК до объектива, H – высота установки ВК.

Размер "слепой" зоны в вертикальной плоскости также увеличивается с увеличением фокусного расстояния объектива. Для выбора угла наклона ВК должно выполняться следующее условие: на максимальной дальности наблюдения высота контролируемой зоны должна быть не менее роста человека, то есть $h_B > 1,8$ м.

Если используемый объектив и положение оси визирования ВК не обеспечивают уменьшение "слепой" зоны до приемлемых размеров, то камеру следует устанавливать в таком месте, чтобы в эту зону не попадали уязвимые места охраняемого объекта (окна, двери и т.д.).

Таким образом, выбор моделей видеокамер производится по результатам расчета для целевых задач видеоконтроля применительно к выделенным на плане объекта критическим зонам.

Многие видеокамеры идут в сборе с объективами, кронштейнами, при этом корпус многих бюджетных моделей может быть рассчитан на эксплуатацию камеры на улице. При выборе объективов учитывается рассчитанное при выборе зон наблюдения фокусное расстояние. Для помещений с панорамным остеклением и для уличных камер важна

функция автоматической регулировки диафрагмы (АРД) объектива. Разрешение объектива должно быть не хуже разрешения камеры, на которую он будет установлен (особенно это важно для *IP*-камер).

Если *IP*-камера работает с ИК-подсветкой, обязательно наличие в объективе ИК-коррекции – она снижает степень расфокусирования изображения за счет дисперсии при включении или выключении ИК-подсветки видеокамеры.

Гермокожухи для уличных видеокамер имеют подогрев, который требует электропитания. Это должно учитываться при расчёте и выборе блоков питания. Если номинал напряжения питания камеры совпадает с напряжением питания подогрева кожуха, то для электроснабжения камеры и кожуха достаточно одной пары проводов. При несовпадении напряжений питания камеры и подогрева требуется предусмотреть отдельные пары проводов для их питания. Существуют термокожухи со встроенными в них блоками питания с входом на 220 В и выходом на 12 В или 24 В.

Кронштейн для камер в помещениях должен иметь длину, достаточную для того, чтобы установленная на него камера могла быть повернута в нужном направлении наблюдения. При установке ВК на наклонные поверхности желательно использовать модели с 3D-кронштейном, который позволяет правильно ориентировать камеру в пространстве.

Устройства записи видеоинформации

Для выбора устройства записи видеоинформации необходимо учесть ряд факторов:

- количество и тип подключаемых видеокамер;
- количество аудиоканалов;
- разрешение и кадровую скорость видеозаписи;
- расчетные параметры видеоархива для определения количества и ёмкости поддерживаемых жестких дисков (видеорегистраторы не комплектуются жесткими дисками);
- востребованные функции видеоанализа изображения;
- количество и тип видеовыходов для устройств отображения;
- количество подключаемых удалённых АРМ;
- возможность управления *PTZ* камерами.

Указанная информация частично извлекается из требований технического задания на проектирование системы, частично является результатом предварительного выбора видеооборудования.

Скорость записи (*recording frame rate*), или кадровая скорость, измеряется в количестве кадров в секунду (или *fps* - *frames per second*), задается при настройке регистратора в соответствии с ТЗ. Для отдельных каналов записи значение кадровой скорости может определяться требованиями модулей видеоанализа. Как правило, кадровая скорость для

систем безопасности имеет диапазон от 1 до 25/30 кадров в секунду. Этот показатель говорит о производительности системы и непосредственно влияет на плавность движения объектов контроля на видеозаписи.

Кадровая скорость влияет и на решение задачи, стоящей перед конкретной видеокамерой (обнаружение, распознавание и идентификация). Например, короткий фрагмент записи запечатлел проходящего преступника, однако из-за низкой скорости записи в нём может не оказаться такого кадра, в котором преступник посмотрел в сторону видеокамеры. По записи невозможно будет сделать его фотопортрет для идентификации, но будет возможно обнаружение и распознавание (определение примет) преступника. Поэтому для выбора кадровой скорости записи видеоинформации принято руководствоваться следующими экспертными установками:

- запись 60 кадров в секунду рекомендуется при съёмке быстро движущегося автотранспорта на магистралях;
- запись 25/30 кадров в секунду рекомендуется при съёмке потоков автотранспорта, особо важных участков объекта, а также для решения задачи идентификации;
- запись 12 кадров в секунду рекомендуется при съёмке помещений объекта охраны, пешеходных зон, а так же для решения задачи распознавания;
- запись 6 кадров в секунду рекомендуется для областей с малой динамикой событий: парковок и дворов, а также для решения задачи обнаружения объектов.

Таблица 9 – Для определения размера видеоархива записи при потоковом алгоритме сжатия видеоинформации H.264

Разрешение видеокамеры		Размер видеоархива в расчете на одну видеокамеру на 30 дней хранения, (Гб)		
		при 6 кадр/с	при 12 кадр/с	при 25 кадр/с
1Мп	1280×720	120	240	500
1,3Мп	1280×1024	160	330	680
2Мп	1920×1024	270	540	1200
3Мп	2048×1536	390	780	2000
4Мп	2560×1440	507	1100	2400
5Мп	2560×1920	650	1300	3000

Далее необходимо произвести расчет ёмкости жестких дисков для хранения архива записей с учетом количества камер, их разрешения, кадровой скорости, длительности записи, применяемых для оцифровки и сжатия видеоинформации алгоритмов (кодеков). Кроме того, на степень

компрессии данных влияет наличие мелких деталей на изображении, а также динамики объектов в рамках сцены.

Для определения размера видеоархива существуют расчетные методики для аналогового и сетевого оборудования, а также эмпирические таблицы, которые составляются экспертами по организации видеосистем (в качестве примера см. таблицу 9).

Каждый тип устройств записи предполагает организацию видеоканала с использованием своего набора возможных способов соединения регистратора с видеокамерой. Необходимо учитывать и ограничения на протяженность коммуникаций в зависимости от способа организации видеоканала (таблица 10).

Таблица 10 – Для учета ограничения на протяженность коммуникаций в зависимости от способа организации видеоканала

Линия связи для организации видеоканала	Предельная дальность передачи сигнала для различных технологий, м			
	Аналог CVBS	IP	AHD, TVI	CVI
Коаксиальный кабель 75 Ом (омеднённая сталь)	70	–	200	200
Коаксиальный кабель 75 Ом (медь)	200	устарел	500	500
Приёмопередатчики по витой паре 3 категории	2000	–	500	–
Витая пара 5 категории (UTP) по Ethernet	–	$100 \times N^*$	–	–
Оптоволокно по Ethernet (1000BASE-FX)	–	2000	–	–
Оптоволокно по Ethernet (1000BASE-LX)	–	5000	–	–

* – количество коммутаторов в линии связи с использованием кабеля UTP.

Устройства записи отличаются количеством и ёмкостью устанавливаемых в него жестких дисков. Для выбранного устройства записи должна быть предусмотрена возможность организации видеоархива с ёмкостью большей, чем было рассчитано ранее. При выборе в качестве устройства записи гибридного (HVR), сетевого (NVR) *stand-alone* видеорегистратора или регистратора на базе видеосервера (для крупных IP-систем) можно руководствоваться представленной сравнительной таблицей 11.

Если общая ёмкость жестких дисков, устанавливаемых в выбранное устройство записи, меньше рассчитанной ранее ёмкости видеоархива, то возможно её увеличение, применением устройств хранения DAS (*Direct*

attached storage) или *NAS (Network attached storage)* при условии, что выбранное устройство записи поддерживает работу с ними.

Таблица 11 – Для сравнения различных реализаций устройств записи

Функция	<i>HVR</i>	<i>NVR</i>	ПК (сервер)+ПО
Количество каналов	До 16, иногда до 28	До 80, иногда до 300	До 300, объединение в кластер
Количество <i>HDD</i>	До 4 + <i>DAS</i>	До 12, иногда до 45 + <i>DAS</i>	До 16, иногда до 28
Видеоанализ	минимум	средние возможности	максимум
Количество удалённых АРМ	10; эффективно 1..3	20; эффективно 1..5	определяется параметрами ПК при заказе
Поддержка стандартов	<i>CVBS/IP/TVI/CVI/AHD</i> в разных сочетаниях	<i>IP</i>	<i>IP</i>
Возможности расширения	отсутствуют	есть	существенные

Таким образом, на основе анализа устройств записи рекомендуется выполнить следующие действия:

- определить необходимость видеоанализа изображения для решения конкретных задач (распознавание автомобильных номеров или лиц, пересечения границ, видеодетекторов дыма или оставленных предметов и пр.) и набор программных модулей для их выполнения;
- выбрать тип устройства видеозаписи (*DVR / NVR / HVR* или ПК), учитывая количество камер, их тип (*CVBS/IP/TVI/AHD/CVI*) и разрешение, требуемые длительности и режимы записи, поддержки требуемой емкости архива, возможности организации постов наблюдения, наличия требуемых функций видеоанализа и других;
- определить модели устройств записи, количества и модели жестких дисков к ним для хранения видеоархива;
- при необходимости выбор устройств хранения информации **DAS** или *NAS* для увеличения емкости видеоархива.

По требованиям технического задания к количеству постов наблюдения необходимо скорректировать сформированную ранее структурную схему функциональной ПСБ: указать монтажное оборудование для реализации способа организации видеоканала (выбор линии связи), а также устройства управления видеокамерами и записи (пульты для *PTZ*-камер, видеорегистраторы, устройства хранения информации). Отметить расстановку выбранных элементов на плане объекта.

Программное обеспечение

Если в качестве устройства записи в сетевой видеосистеме принимается сервер, необходимо выбрать для него программное обеспечение (ПО) и конфигурацию. В рамках учебного проекта для решения указанных вопросов следует пользоваться информацией с сайтов отечественных разработчиков программных платформ для видеонаблюдения (ITV, DSSL, Macroscop и других). Поскольку проект предусматривает наличие экономической части, для определения стоимости программных продуктов принимаются во внимание следующие положения.

Производители ПО могут поставлять разные виды основных лицензий, которые имеют ограничения по количеству камер в системе, наличию и ассортименту интеллектуальных модулей видеоаналитики, количеству поддерживаемых АРМ, количеству серверов в системе.

Кроме основных, предлагаются дополнительные лицензии для поддержки различных функций, которые поставляются в виде опций. К ним относятся программные модули видеоанализа, поддержка камер Fisheye, а иногда и *PTZ*, поддержка звука, модули интеграции с различными программными продуктами СКУД и ОПС.

Как правило, стоимость базового ПО формируется, исходя из количества видеоканалов (лицензий) в видеосистеме. Одна лицензия предоставляет возможность подключения одной IP-камеры и обработки видеопотока от нее.

Наиболее распространены модели бюджетных камер, формирующие на выходе 2 видеопотока: основной максимального разрешения (для записи) и дополнительный малого разрешения, который используется для построения мультиэкрана или для передачи на мобильные телефоны. В таких случаях покупается одна лицензия на ПО для работы с обоими потоками, так как дополнительный поток не несёт нового контента и используется как вспомогательное средство.

Для построения больших систем, в том числе, с видеоаналитикой, могут использоваться IP-камеры высокого ценового диапазона, которые могут выдать более двух потоков высокого разрешения. В этом случае вопрос покупки лицензий зависит от политики фирмы-разработчика ПО. Как правило, обычно каналы записи и модули аналитики имеют свои лицензии. Лицензии на ПО для поддержки АРМ у разных фирм также приобретаются на разных условиях.

Таким образом, количество основных лицензий на ПО определяется количеством каналов записи (количеством IP-камер), а количество и ассортимент дополнительных лицензий определяется количеством камер в системе, по которым есть потребность в разных видах видеоаналитики и

дополнительных функциях (например, для работы с *PTZ*-камерами, с панорамными, в том числе, многоматричными, камерами) [12-14].

По указанным принципам производится выбор ПО для сетевой СОТ учебного объекта охраны. Следует учитывать, что если при создании проекта оговорена возможность расширения его до определенного масштаба, то это также необходимо учитывать при выборе основных лицензий, которые, как правило, имеют ограничение на максимально возможное количество поддерживаемых *IP*-камер.

Для работы выбранного ПО с необходимым набором возможностей нужно подобрать конфигурацию сервера. Для этого необходимо изучить документацию на ПО (она доступна на сайте производителя), в которой указаны минимальные системные требования к серверам. Как правило, на сайтах производителей есть «калькулятор», который по заданным параметрам программы (количество видеоканалов, параметры записи, количество используемых модулей видеоаналитики, количество АРМ, количество видеопотоков от одной камеры и т.п.) даёт данные о минимальных системных требованиях к конфигурации сервера(ов) (процессор, оперативное запоминающее устройство (ОЗУ), жесткий диск (*HDD*), скорость сетевой карты (для передачи данных от сервера в сеть: 1000 Мб/с – для большого количества камер, 100 Мб/с – для малого), иногда и видеокарты (при повышенной нагрузке по декодированию видеопотока для крупных систем).

Видеоаналитика распознавания автомобильных номеров или лиц людей связана с распознаванием образов, поэтому есть определенные требования к размеру и разрешению изображения объектов распознавания. Эти требования указаны в сопроводительной документации к модулям видеоаналитики, которая доступна на сайте производителя. Для *IP*-камер, формирующих изображение для реализации, указанной серверной видеоаналитики, необходимо произвести дополнительную проверку, удовлетворяет ли качество изображения требованиям выбранного программного модуля.

Если изображение имеет недостаточное разрешение, то нужно изменить некоторые параметры: разрешение камеры, угол обзора объектива, расстояние от камеры до объекта. При необходимости производится замена или объектива, или камеры (выбирается с более высоким разрешением), или места её установки.

Видеоаналитика распознавания образов накладывает ограничения и на ракурс съёмки, который зависит от расположения камеры относительно объекта распознавания, предельных углов в вертикальной и горизонтальной плоскостях, с которых может вестись наблюдение. Нарушение данных требований может привести к тому, что модуль видеоанализа будет распознавать объекты с меньшей достоверностью или не будет распознавать совсем. Если выбранное на более раннем этапе

проектирования расположение камер по зонам контроля не соответствует требованиям программ распознавания, то необходимо изменить расстановку соответствующих камер.

Управление поворотными видеокамерами

Для поворотных видеокамер (*PTZ* камер) необходимо выбрать устройства управления, которые могут быть интегрированы в устройства записи (видеорегистраторы) или реализуются в виде отдельных пультов.

Протокол управления *PTZ* камерой и протокол, поддерживаемый пультом, должны совпадать. Из-за различий реализаций протоколов управления разными производителями возможно отключение отдельных функций *PTZ* камер. По этой причине рекомендуется использовать поворотные камеры и пульты управления от одного производителя.

Указанное замечание справедливо для оборудования на базе аналоговых технологий (как для уходящего с рынка систем безопасности традиционного композитного (*CVBS*) видео, так и современного видеооборудования высокой четкости (*HD*), независимо от аппаратной реализации регистратора (*stand alone* или на базе сервера), а также частично для сетевых систем, в которых устройство записи и управления реализуется в виде *stand-alone NVR* регистратора.

Управление поворотными *IP*-камерами выполняется от *NVR* или ПК через программу или специализированный пульт, подключаемый к устройству записи. Функция управления поворотными камерами не всегда входит в комплект поставки специализированного ПО для серверного решения, а может продаваться в виде программного модуля как отдельный товар за дополнительную плату. В этом случае необходимо заложить в спецификацию название необходимого программного модуля [15, 16].

Пульт управления должен находиться в помещении охраны, где расположены и мониторы наблюдения. Необходимо учитывать, что для управления *PTZ* камерами через интерфейс *RS485* (для аналоговых технологий) длина линии связи от пульта или устройства записи до поворотной камеры не должна превышать 1000 метров. Управление поворотными камерами возможно также с АРМ или смартфонов, удалённо подключенных к устройству записи через компьютерную сеть.

Устройства отображения

По требованиям технического задания и в соответствии с составленной ранее структурной схемой функциональной подсистемы видеонаблюдения необходимо выбрать способы и устройства вывода изображения для заданного количества постов наблюдения. Вывод изображения может производиться на:

- мониторы, подключённые к устройствам записи;
- ПК с АРМ, которые получают информацию от устройств записи по компьютерной сети *Ethernet*;

- мобильные устройства (планшеты, смартфоны), которые получают информацию от устройств записи по компьютерной сети с беспроводным соединением.

Количество мониторов зависит от количества устройств записи и количества у них видеовыходов. Мониторы подключаются к устройствам записи при помощи разных интерфейсов:

- *VGA* — аналоговый интерфейс, используется для вывода видеоизображения. Устаревает, т.к. производители мониторов переходят на более современные интерфейсы;
- *DVI* — интерфейс имеет модификации с аналоговой и цифровой передачей сигнала, используется для вывода видеоизображения. Близок по своим параметрам к *VGA* и редко используется в оборудовании видеонаблюдения, т.к. производители мониторов переходят на более современный интерфейс *HDMI*;
- *HDMI* — современный цифровой интерфейс, используется для вывода видеоизображения и звука;
- *DisplayPort* — по возможностям аналогичен *HDMI*. Он редко используется в аппаратуре видеонаблюдения.

Монитор и выход устройства записи для передачи видеoinформации на монитор должны иметь одинаковый интерфейс.

Чем большее количество камер выводится на монитор, тем большего размера он должен быть. На размер влияют и требования эргономики, связанные с расстановкой мониторов, количеством операторов, расстоянием от оператора до мониторов (см. требования ГОСТ в Приложении 2).

Так как длина кабеля для подключения монитора не превышает 10-15 метров, то мониторы должны располагаться в непосредственной близости от устройств записи.

Удаленные АРМ и мобильное наблюдение

Для организации удалённых от устройств записи постов наблюдения обычно используют ПК с АРМ. Они получают информацию от устройств записи по компьютерной сети Ethernet. Выбор конфигурации ПК производится по рекомендациям производителя используемого устройства записи, которые указаны в инструкции на него. Программа работы АРМ может поставляться бесплатно или на платной основе.

Как правило, для небольших объектов бесплатное ПО для работы АРМ идет в комплекте с устройствами записи типа видеорегистратора stand alone (на *DVD* в комплекте с устройством записи или загружается с сайта производителя), оно может использоваться на АРМ, но с простым функционалом (только смотреть).

В сетевых системах для крупных объектов, в дополнение к базовому ПО для обработки и записи данных от *IP*-камер, на платной основе приобретаются программы для удалённых АРМ. Такие программы

учитывают наличие видеоаналитики, поддерживают права доступа к системе (кто и что видит и может), обеспечивают расширенный функционал для мониторинга контролируемых объектов.

В случае использования для записи сервера с ПО необходимо удостовериться, что использование удалённого АРМ разрешено приобретённой лицензией на ПО.

Удалённые АРМ часто могут работать с несколькими устройствами записи (функция *CMS – Central Monitoring Station*). Это используется для вывода изображений от нескольких устройств на один монитор ПК. В силу конкуренции и отсутствия стандартизации в этом вопросе практически всегда для совместной работы в одной программе используются устройства, выпущенные одним производителем. С использованием *CMS* возможно объединение на одном мониторе (или видеостене) информации от разных типов устройств: *NVR*, *HVR* и *IP*-камер. Возможность используется для объединения различных видеоподсистем в рамках одного поста наблюдения.

Мобильное наблюдение с использованием смартфонов и планшетных компьютеров обычно применяется как дополнение к наблюдению через мониторы или удалённые АРМ. При мобильном наблюдении в настоящее время возможности сводятся к основным функциям прямого контроля текущей ситуации, простого просмотра информации из видеоархива и управления поворотной камерой.

Электроснабжение и монтаж элементов системы

Для устройства записи, коммутаторов компьютерных сетей и мониторов, как правило, используется питание от электросети с напряжением 220 вольт. Для видеокамер необходимо выбрать блоки питания в соответствии с указанными в технической документации параметрами. При наличии требований по бесперебойной работе системы в случае отключения основного электропитания необходимо выбрать систему бесперебойного питания и рассчитать требуемую для этого ёмкость аккумуляторных батарей (АКБ) по методике, изложенной в одноименном подразделе данного пособия по проектированию ОПС.

Для всех элементов видеосистемы, по которым требуется обеспечить бесперебойную работу, необходимо определить их параметры питания и сгруппировать по типам (переменное или постоянное напряжение) и значениям напряжения питания.

В результате выполненных работ необходимо скорректировать содержание графических материалов проекта. На плане расстановки оборудования требуется отобразить места установки всех рассмотренных выше элементов СОТ в соответствии с требованиями нормативных документов по выполнению графических обозначений элементов систем безопасности. Должны быть обозначены зоны видеоконтроля для всех камер. Для пояснения размеров и конфигураций зон видеоконтроля и

«мёртвых» зоны некоторых видеокамер разрабатывают дополнительные наглядные материалы.

Если используются видеокамеры и устройства записи на базе IP технологий, необходимо выбрать коммутирующее оборудование компьютерных сетей.

Построение IP видеосистемы

Итак, видеосистема, в состав которой входят IP-камеры, компьютеры или сетевые видеорегистраторы, для передачи информации использует локальную компьютерную сеть.

Одним из основных устройств, используемых для построения компьютерной сети, является сетевой коммутатор или свичер (SW). Коммутаторы объединяют и передают в различных направлениях информацию от всех IP-устройств: IP-камер, компьютеров АРМ, устройств записи. Устройства подключаются к коммутатору через специальные интерфейсы, которые часто называют портами коммутатора. К коммутатору обычно подключают устройства 4-х парным кабелем UTP категории 5е с разъёмами RJ45.

Коммутаторы, используемые в настоящее время в СОТ, имеют порты с максимальной скоростью передачи информации 100 Мбит/с и 1000 Мбит/с. В документации и описаниях на коммутатор скорость передачи данных может обозначаться следующим образом:

- для 100 Мбит/с: *Fast Ethernet*, 100 Мбит/с, 100BASE-TX или IEEE100BASE-TX
- для 1000 Мбит/с: *Gigabit Ethernet*, GE, GbE, 1GigE, 100BASE-TX или IEEE100BASE-TX

Для подключения IP-камеры обычно используют порты со скоростью передачи 100 Мбит/с. Интерфейс с пропускной способностью 1000 Мбит/с обычно используется для:

- соединения между 2-мя коммутаторами, по которому будет передаваться объединённый трафик от всех подключённых IP-камер;
- подключения устройства записи;
- подключения компьютеров с АРМ.

Потоки информации от всех IP-камер передаются на устройство записи, а значит, на линии связи, идущей к видеорегистратору или серверу, все потоки информации суммируются.

Для выбора моделей коммутаторов в системе необходимо рассчитать пропускную способность компьютерной сети (трафик от видеокамер), то есть объём информации, передаваемой через компьютерную сеть за определенное время. Объём трафика зависит от таких параметров, как разрешение ВК, кадровая скорость, кодек, динамика снимаемой сцены, наличие функций видеоанализа и других.

Для расчётов пропускной способности компьютерной сети и размера видеоархива для сетевой видеосистемы возможно использование усредненных данных. В таблице 12 приведены данные по трафику за одну секунду (битрейту) при кадровой скорости 25 кадров в секунду при среднем уровне компрессии для наиболее распространенных алгоритмов сжатия.

Таблица 12 – Данные по трафику за 1 секунду при кадровой скорости 25 кадров в секунду при среднем уровне компрессии

Разрешение IP-камеры		Трафик, Кбит/с		
		H.265	H.264	MJPEG
1Мп	1280×720	3 019	4 783	14 557
1,3Мп	1280×1024	3 915	6 132	18 345
2Мп	1920×1024	6 027	8 417	31 045
3Мп	2048×1536	9 046	12 568	45 037
4Мп	2560×1440	12 055	16 743	51 856
5Мп	2560×1920	15 074	19 600	71 967
6Мп	3072×2048	18 093	22 816	86 896

В учебном проекте можно оговорить, что пользовательские данные (информация от IP камер и данные различных программ, в зависимости от специфики объекта охраны, например, таких как 1С, SQL, сетевые игры и прочие) должны составлять не более 80% пропускной способности соединения. Таким образом, если суммарный трафик от IP-камер не превышает 80 Мбит/с, то для соединения коммутатора с ПК или NVR используются порты со скоростью 100 Мбит/с. В противном случае используются порты со скоростью 1000 Мбит/с.

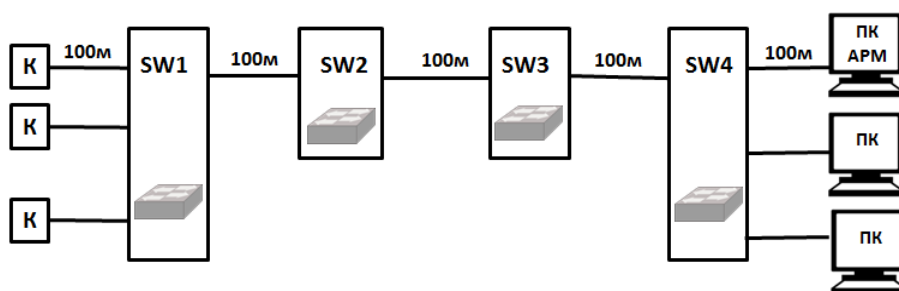


Рисунок 3 – Пример формирования локальной компьютерной сети с каскадным подключением коммутаторов IP-видеосистемы

Длина одного участка UTP кабеля по стандартам *Fast Ethernet* или *Gigabit Ethernet* не может превышать 100 метров. Если необходимо передать видеопоток на большее расстояние, то применяют следующие способы.

1) Установка коммутатора на небольшое количество портов, который получает информацию по кабелю UTP и ретранслирует её ещё на 100 метров. Такой способ оправдан для передачи информации на расстояния 200...500 метров (рис.3).

2) Коммутаторы с портами для *SFP* модулей, к которым подключается оптоволокно. Длина линии может составлять несколько километров.

В рамках учебного проекта соединения *Fast Ethernet* и *Gigabit Ethernet* выполняются кабелем витая пара (*UTP*) категорий 5е или одномодовыми волоконно-оптическим кабелем. При использовании оптического волокна определяется необходимое количество *SFP*-модулей (из расчета по два модуля на один участок оптоволоконного соединения). Для *UTP* определяется необходимое количество разъёмов *RJ45* (из расчета по два разъема на один участок проводного соединения).

Power over Ethernet

IP-камеры, подключенные кабелем *UTP*, могут по нему получать питание по технологии *Power over Ethernet (PoE)* от коммутатора. Есть разные стандарты *PoE*, отличающиеся мощностью, подаваемой от коммутатора на *IP*-камеру (таблица 13):

Таблица 13 – По стандартам *PoE*

Стандарт	Максимальная мощность на <i>IP</i> -камеру	Название
<i>IEEE 802.3af-2003</i>	15 Вт	<i>PoE</i>
<i>IEEE 802.3at-2009</i>	25,5 Вт	<i>High PoE, Poe+</i> или <i>PoE plus</i>

Если потребление *IP*-камеры превысит мощность, которую выдаёт порт в соответствии со стандартом *PoE*, то коммутатор автоматически отключает подачу питания поданному порту. Обязательными условиями работоспособности являются:

- поддержка *PoE* как *IP*-камерой, так и коммутатором, к которому она подключена;
- мощность потребления одной *IP*-камеры не превышает мощность, выдаваемую одним портом коммутатора;
- суммарная мощность, потребляемая *IP*-камерами, не превышает мощность, которую коммутатор может передать по стандартам *PoE*.

При необходимости бесперебойной работы *IP*-камер, питающихся по *PoE*, необходимо обеспечивать резервное питание для коммутатора.

Таким образом, выбор коммутаторов непосредственно связан с формированием топологии сетевой структуры всей видеосистемы. Поэтому на данном этапе проектирования рекомендуется выполнить следующие действия:

- на плане объекта сделайте расстановку коммутаторов с учётом оговоренных ограничений по дальности передачи данных;
- выполнив схематическое соединение оборудования, определите количество задействованных портов на каждом коммутаторе и их

параметры (скорость соединения и способ организации видеоканала - UTP или оптоволокно);

- подсчитайте количество, тип и скорость используемых портов;
- выберите с использованием поисковых систем модели коммутаторов, подходящих полученным требованиям;
- скорректируйте структурную схему взаимодействия элементов системы, которая поясняла бы выбранную организацию сети.

Кабель для систем видеонаблюдения

После выбора и размещения на плане объекта основных элементов видеосистемы (камер, устройств записи, мониторов, элементов питания и компонентов компьютерной сети) необходимо обеспечить их соединение: выбрать марки и количество кабельной продукции.

Для проводного соединения элементов СОТ используются коаксиальный кабель при подключении аналоговых и HD-видеокамер, витая пара - для создания компьютерной сети, силовой кабель - для подключения элементов видеосистемы к блокам питания с учётом условий прокладки в помещениях или на улице. Учитывая расстановку элементов видеосистемы, необходимо определить количество расходных материалов каждого вида.

В соответствии с ГОСТ Р 51558-2014 основное электропитание средств СОТ должно осуществляться от сети переменного тока частотой 50 Гц номинальным напряжением 220 В. В рамках проекта считаем, что электропитание устройств от сети 220 В, находящихся в зданиях, рядом с электрощитами или розетками будет подключаться штатными кабелями питания, поставляемыми в комплекте поставки оборудования. Для устройств, находящиеся на удалении от типичных мест нахождения розеток питания 220 В, необходимо выбрать тип и сечение кабеля.

Выбор сечения кабеля зависит от суммарной силы тока потребителей и материала, из которого изготовлен кабель. Информация о сечении силового кабеля для напряжения 220 В приведена в таблице 14.

Таблица 14 – Для выбора сечения кабеля питания элементов системы

Сечение токопроводящей жилы, мм ²	Допустимый ток, А			
	алюминий		медь	
	Ток, А	Мощность, кВт	Ток, А	Мощность, кВт
1,5	12	2,7	19	4,1
2,5	20	4,4	27	5,9
4	28	6,1	38	8,3
6	36	7,6	46	10,1

Наиболее часто в видеосистемах используются силовой кабель серий: ПВС, ВВГ, ШВВП, NYM.

Наиболее распространенные марки коаксиального кабеля: РК-75, RG59/U, RG6/U и RG11/U. Центральная жила коаксиального кабеля выполняется из меди или её сплавов. Такой кабель имеет хорошие характеристики по затуханию видеосигнала, но достаточно высокую стоимость. В случае ограниченного бюджета возможно использование кабеля со стальной жилой с медным покрытием (сталь, плакированная медью), в этом случае жилу называют омедненным проводом (*BCW, Bare Copper Weld*). Такой кабель имеет высокое затухание и обеспечивают передачу видеосигнала на расстояния не более 50-70 метров.

Затухание видеосигнала в коаксиальном кабеле зависит от параметров материалов, диаметра центральной жилы, изоляции кабеля и его длины. Чем длиннее нужно выполнить линию соединения, тем с меньшим затуханием необходимо использовать кабель.

Необходимо подсчитать суммарную длину кабеля каждого типа. Кабель поставляются бухтами разной длины: по 100, 200, 250 и 500 метров. Кабель витая пара *UTP* и *FTP* обычно имеет фасовку в бухты по 305 метров. Количество необходимого кабеля округляется в большую сторону с учётом выбранного метража упаковки. Если метраж упаковки кабеля неизвестен, считаем его равным 100 метрам.

Для подключения видеокамер может использоваться комбинированный кабель. Он специально предназначен для передачи видеосигнала с одновременной подачей питания для видеокамер и подогрева термокожухов, подключения линий управления по *RS-485*. Он представляет собой коаксиальный кабель или кабель витой пары и несколько проводов сечением 0,35-1,5 мм², объединённые общей оболочкой. Комбинированный кабель удобен в случае, если блоки питания и пульты управления *PTZ*-камерами находятся рядом с устройством записи.

Наиболее часто в видеосистемах используются комбинированный кабель серий: КВК, ККСВ, ККСВП.

При формировании линий соединения на улице используется кабель с указанием возможности его применения в таких условиях. Он устойчив к воздействию неблагоприятных климатических факторов (морозов, влаги, прямого солнечного света) и обеспечивают надёжное соединение в течение нескольких лет.

При прокладке кабеля навесным способом (между соседними зданиями или на столбах по открытым пространствам) нужно применять марки с наличием в их конструкции металлического троса. Трос интегрирован в конструкцию кабеля и обеспечивает его механическое крепление к точкам подвеса, а также несущую способность конструкции.

Для прокладки под землей применяют специальные виды кабеля, укладываемого непосредственно в грунт. Внешняя оболочка такого кабеля содержит защитные материалы, позволяющие его можно укладывать прямо в траншею.

Подключение мониторов к устройствам записи в непосредственной близости друг от друга по интерфейсам *VGA*, *DVI* и *HDMI* производится кабелем, идущими в комплекте поставки данного оборудования.

Сформированная в итоге спецификация оборудования должна включать: название моделей элементов видеосистемы, производитель, количество оборудования, его основные характеристики.

5.3.3 Порядок проектирования системы контроля и управления доступом

Общие положения по проектированию СКУД

В процессе создания СКУД определяются задачи, функции и архитектура системы применительно к конкретному объекту, уточняются параметры основных элементов структурной схемы с последующим выбором количества и моделей необходимых программно-технических средств. Можно рекомендовать следующий порядок проектирования СКУД как функциональной подсистемы КСБ:

- определение задач системы и её основных параметров таких, например, как количество пользователей, дальность считывания кода идентификатора, количество точек доступа, контроль в одну/две стороны, наличие и количество АРМ;
- определение функций, необходимых в СКУД для решения задач;
- выбор типа системы (локальная/сетевая/смешанная или комбинированная) и ее архитектуры;
- определение мест расположения зон доступа, точек доступа и требований к ним;
- выбор идентификаторов, носителей кодов доступа, используемых для идентификации, и считывателей;
- выбор контроллеров;
- выбор интерфейсов соединения контроллеров системы и соединения контроллеров со считывателями;
- выбор ПО (для сетевых и смешанных систем);
- выбор исполнительных устройств;
- выбор элементов питания и кабеля для линий соединений;
- выбор элементов локальной вычислительной сети (ЛВС) для СКУД, использующих связь по Ethernet, а также облачные сервисы [17].

СКУД предназначена для ограничения и регистрации доступа людей (персонала, посетителей, клиентов), транспорта и других объектов в помещения, здания и территории объекта. Ограничение доступа означает предотвращение проникновения нежелательных лиц на охраняемую территорию и помещения, обеспечение сохранности материальных и интеллектуальных ценностей. Регистрация доступа предполагает распознавание того лица, которое получает доступ, и фиксацию времени

предоставления доступа (типовым примером может служить проходная со СКУД с функцией учета рабочего времени).

Поэтому в качестве основных функций СКУД можно рассматривать следующие [3]:

а) предоставление или запрет допуска в контролируемую зону лиц, в зависимости от имеющихся у них права прохода;

б) управление режимом прохода в контролируемые зоны, дистанционное управление состоянием исполнительных устройств;

в) ведение автоматизированного учета пропусков (идентификаторов) и хранение в базе данных информации об их владельцах;

для сетевых систем:

г) протоколирование событий в системе, включая изменение режимов работы оборудования, программного обеспечения и фиксацию действий операторов, работающих с системой;

д) ведение учета рабочего времени, формирование отчетов о событиях;

е) обеспечение возможности дистанционной визуальной идентификации владельцев пропусков.

Архитектура системы и интерфейсы связи

Выбор архитектуры СКУД определяется масштабом объекта, количеством контроллеров в системе и расстоянием между ними, наличием и количеством в системе компьютеров с АРМ. Для связи контроллеров используются интерфейсы RS-485 или Ethernet. Для связи контроллеров с компьютерами применяются интерфейсы RS-232, USB или Ethernet [2, 18].

Для объектов в пределах одного здания с общей длиной линий связи не более одного километра возможно применение контроллеров, связанных в единую сеть через интерфейс RS-485. При необходимости подключения таких систем к ПК применяют различные преобразователи интерфейсов: RS485-RS232, RS485-Ethernet или RS485-USB. Пример такой системы представлен на рисунке 4.



Рисунок 4 – Схема системы с линиями связи по интерфейсу RS-485

Для объектов в больших зданиях или комплексов зданий, а также для территориально распределенных систем с удалением в пределах города или

страны обычно разрабатываются архитектуры СКУД на основе компьютерных сетей и применяются контроллеры с интерфейсом Ethernet. По сравнению с сетевыми видеосистемами, СКУД передают небольшое количество данных, поэтому создание отдельных ЛВС для них нецелесообразно. Для СКУД возможно использование уже существующих компьютерных сетей. Схема системы на основе интерфейса Ethernet представлена на рисунке 5.

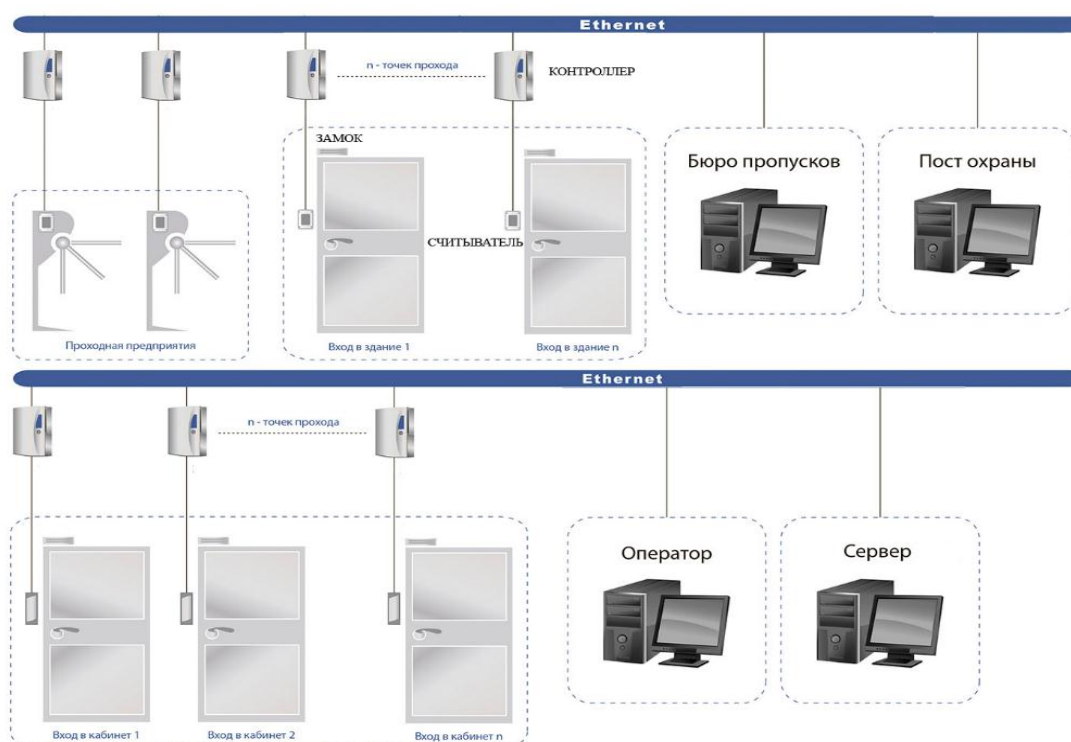


Рисунок 5 – Схема системы с линиями связи по интерфейсу Ethernet

Возможно и сочетание архитектур, когда в пределах небольших зданий создаётся система на базе RS485, а несколько таких зданий объединяются посредством сети Ethernet и облачных сервисов. Пример такого соединения показан на рисунке 6.

В схемах со смешанной архитектурой объединяющим элементом является ПК. Как правило, компьютер не содержит для связи интерфейс RS-485, поэтому для подключения к нему контроллеров используются преобразователи интерфейсов (такие, например, как RS485/USB, RS485/Ethernet), которые служат для обеспечения взаимодействия контроллеров доступа подсистем, соединённых на базе RS-485, в рамках единой сети Ethernet [18, 19].

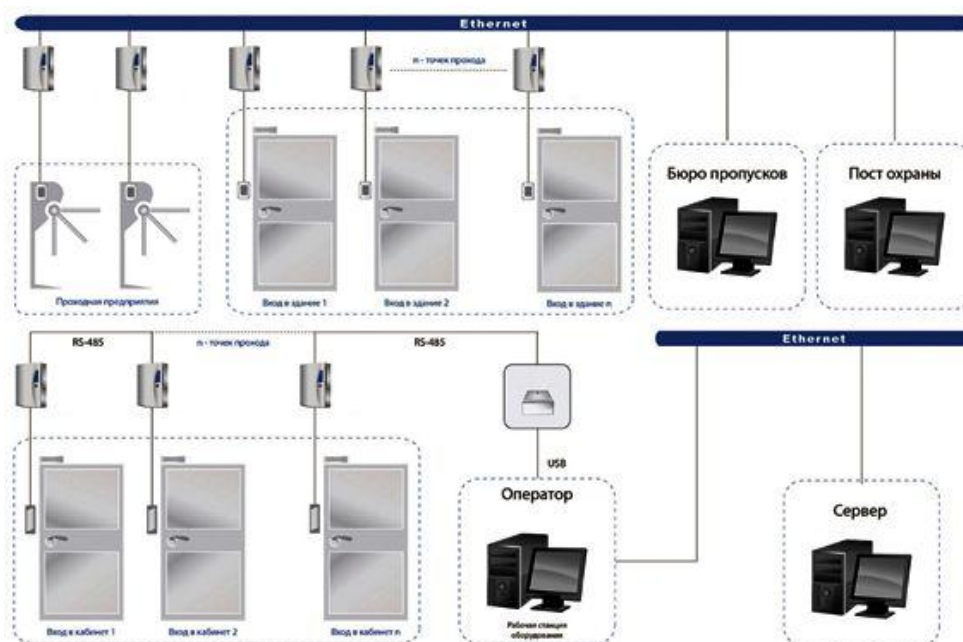


Рисунок 6 – Схема системы с линиями связи по интерфейсам RS-485 и Ethernet

При создании систем со смешанной архитектурой их производители формируют специализированные серии оборудования, в которые входят контроллеры с разным набором параметров, преобразователи интерфейсов и программное обеспечение. В пределах серии оборудования обеспечивается полная совместимость её компонентов [19, 20, 21].

Программное обеспечение

Для централизованного управления СКУД территориально распределенных объектов, получения сводных отчётов о событиях на контролируемых объектах, необходимости учёта рабочего времени, интеграции с программами 1С или другими системами обычно используют ПК с установленным на него программным обеспечением.

На объектах с большим количеством персонала, при наличии гостевых посетителей необходимо создание бюро пропусков. Важными функциями ПО в этом случае могут быть следующие:

- фотоидентификация и графическое оформление пропусков – нанесения фотографий и дополнительной информации на идентификаторы;
- автоматическая синхронизация списка сотрудников в СКУД по внешней базе данных существующей корпоративной системы;
- работа с гостевыми идентификаторами посетителей;
- автоматическое сканирование и распознавание документов при выдаче временного пропуска посетителю;
- управление системой через графический интерфейс с электронными планами объекта.

В этом случае необходимо предусмотреть в системе компьютер с соответствующим АРМ, подключённым к считывателю идентификаторов. Для реализации некоторых функций могут быть необходимы сканер для документов, цифровая камера или фотоаппарат, специальный принтер для нанесения графической информации на идентификатор. Необходимо уточнить наличие необходимых интерфейсов для подключения указанного оборудования и его поддержку программными модулями.

ПО может строиться по модульному принципу, при котором базовая версия обеспечивает основные операции по работе с базой пользователей, управлению и настройке контроллеров локально или удалённо, определению прав и расписаний доступа пользователей и операторов. Другие функции могут реализовываться программными модулями, поставляемыми за дополнительную плату.

Проектируемая система должна обеспечивать требуемый техническим заданием функционал. Поэтому ПО должно содержать необходимый набор модулей.

Идентификатор и носитель кодов доступа

В качестве идентификатора может использоваться код, считанный из разных носителей или набранный на клавиатуре, а также ряд биометрических признаков человека (отпечаток пальца, рисунок сетчатки или радужной оболочки глаза, изображение лица и другие).

Режим и способ идентификации во многом зависят от выбора носителя кода, удобства его использования и определяют защищенность системы от злоумышленников, стоимость СКУД.

На объектах, где требуется высокий уровень защищенности, как правило, используют двойную идентификацию одного пользователя по обязательному предъявлению двух разных идентификаторов (например, карты и набора кода на клавиатуре, или отпечатка пальца и карты).

Носитель идентификатора (кода доступа) должен удовлетворять требованиям ТЗ по устойчивости к подделке, износу и обладать приемлемой стоимостью.

Далее рассматриваются наиболее распространенные контактные и бесконтактные материальные носители для предъявления идентификаторов на объектах различного масштаба.

Контактная память Touch Memory (ключи Dallas) – класс электронных устройств в металлическом корпусе, который одновременно является электрическим контактом и служит для защиты находящихся внутри микросхем. Достоинствами Touch Memory являются небольшой размер, высокая стойкость к механическим повреждениям и коррозии. К недостаткам можно отнести простоту копирования и контактный способ считывания, что снижает пропускную способность системы.

Бесконтактные карты или брелоки (*proximity*) используют радиочастотную технологию идентификации (*RFID*), имеют невысокую

стоимость и удобны в использовании: обеспечивают считывание в течение 0,1 секунды с расстояния от нескольких сантиметров до десятков метров [22, 23]

Бесконтактные карты формата *Em Marin* на данный момент являются наиболее популярным решением в СКУД благодаря широкой номенклатуре считывателей и идентификаторов в сочетании с их низкой ценой [24]. Недостатком является простота копирования и несанкционированного считывания информации с последующим изготовлением дубликата карты, что делает невозможным применение карт *Em Marin* на важных объектах или в системах, где используется функции, связанные с оплатой услуг или хранением персональной информации (транспорт, бесконтактные социальные карты и т.п.).

Серии бесконтактных карт форматов *MIFARE* и *HID* используются в системах с высокими требованиями к безопасности и функциональности. Они отличаются друг от друга разной длиной ключа (*UID*), структурой и ёмкостью памяти для данных, числом циклов записи и чтения информации, алгоритмами шифрования и другими особенностями [23, 25]. В таблице 15 представлены основные параметры наиболее распространенных бесконтактных носителей.

Таблица 15 – Основные бесконтактные карты для организации доступа

Параметры и свойства	<i>Em Marin</i>	<i>Mifare Classic 1K</i>	<i>Mifare Plus</i>	<i>Mifare Plus X2K</i>	<i>HID Prox</i>	<i>HID iCLASS SE</i>
Рабочая частота	125 кГц	13,56 МГц	13,56 МГц	13,56 МГц	125 кГц	13,56 МГц
Длина серийного номера, байт	3	4	7	7	–	–
Наличие памяти, Килобайт	нет	1–4 KB	2–4 KB	2 KB	нет	2–32 KB
Криптографическая защита	нет	Crypto 1	AES	AES128	нет	есть
Защита от копирования	нет	Высокая	Очень высокая	Очень высокая	нет	Очень высокая
Стандарт ISO	–	14443	14443	14443	14443	14443 15693

Выбор носителя идентификатора кода доступа определяется задачей СКУД, требованиями по защищенности и приоритетом той или иной функции. Для СКУД с задачей регистрации достаточно идентификаторов Touch Memory или карт Em Marin. Если основной задачей СКУД является ограничение доступа с защищенностью идентификатора от копирования, то ключей Touch Memory или карты типа Em Marin и других проксимити-карт таких, как HID, Indala, работающих на частоте 125 КГц (LF-карты), будет недостаточно.

Карты HID и Mifare с высокой степенью защиты, работающие на высокой частоте 13,56 МГц (HF-карты), могут использоваться не только как идентификаторы доступа, но и как носители специфических, в том числе, персональных, данных (информация о локальной оплате услуг, о состоянии банковского счета, персональные данные владельца карты и прочее).

Для организации автоматизированных средств управления доступом транспортных средств требуется обратить внимание на дальность считывания информации из идентификатора считывателем. В таких случаях применяются:

- пассивные метки радиочастотной идентификации с рабочей частотой 860-960 МГц и дальностью 0,1-0,7 метров; карточка в форм-факторе банковской карты выдается водителю или ставится в салоне автомобиля;
- активные метки (транспондеры) со встроенным или подключаемым внешним источником питания и дальностью считывания до 100 метров; они устанавливаются в салоне и получают питание от бортовой сети автомобиля.

Биометрические идентификаторы, несмотря на их высокую стоимость, используются в системах с высокими требованиями к уровню защиты.

Выбор носителя кода доступа должен соответствовать пропускной способности каждой точки прохода, оборудованной преграждающими управляемыми устройствами (далее - УПУ), в зависимости от временного режима работы объекта. Под **пропускной способностью** понимается способность средства или системы КУД пропускать через заданную точку доступа определенное число субъектов или объектов доступа в единицу времени (ГОСТ Р 51241-2008, статья 3.23).

Поэтому для обоснования выбора носителя необходимо выполнить ориентировочный расчет пропускной способности системы на границе критической зоны прохода во время максимальной пиковой нагрузки. Например, на крупных объектах важно учитывать, что значительная часть пользователей (сотрудников) имеет единый график работы. При этом максимальная интенсивность движения через проходную и по маршрутам к

ней наблюдается в начале и по окончании рабочего дня. Оборудование СКУД на таких объектах должно быть рассчитано на максимальную нагрузку в пиковые периоды. То есть позволять войти или выйти персоналу предприятия в течение заданного промежутка времени, не создавая задержек и заторов по пути следования.

Длительность сеанса прохода одного человека рассчитывается как сумма временных промежутков отдельных последовательных операций:

- длительность считывания информации с идентификатора;
- время обработки информации и принятия решения о доступе контроллером;
- время срабатывания исполнительного устройства;
- время прохода (проезда) пользователя через точку доступа;
- длительность закрывания двери и восстановления её блокировки.

Таким образом, каждый элемент оборудования СКУД вносит свой вклад в её пропускную способность, в том числе и носитель идентификатора, который непосредственно определяет влияние человеческого фактора на длительность сеанса прохода через границу доступа (задержка при предъявлении носителя пользователем, правильность положения носителя для считывания, время удержания носителя у считывателя, скорость движения пользователя в области точки прохода и прочие его индивидуальные особенности).

Для выбранных элементов необходимо рассчитать длительность сеанса прохода одним пользователем через одну точку прохода. Зная максимальное количество пользователей и пропускную способность одной точки доступа (двери, турникета) системы необходимо рассчитать требуемое количество точек доступа для обеспечения выхода всех пользователей в периоды пиковых нагрузок.

Если выбранное оборудование для точки прохода не обеспечивает рассчитанную пропускную способность, можно увеличить число точек прохода на границе зоны доступа. Если увеличение количества точек прохода затруднено, то необходимо выбрать более быстрый способ идентификации или выбрать модели оборудования с лучшими временными параметрами.

Кроме соответствия техническим параметрам системы, при выборе носителя необходимо учитывать, что способ применения носителя должен быть удобен для его предъявления пользователем. Например, для идентификации транспортных средств удобно использовать бесконтактные идентификаторы с большой дальностью считывания, а не метки со штрих-кодом или контактные ключи Touch Memory.

При выборе типа идентификатора и носителя кода доступа также следует учитывать, что при большом количестве пользователей цена идентификатора существенно влияет на общую стоимость системы и должна приниматься во внимание при финансовых ограничениях на

систему. При использовании биометрических идентификаторов время считывания существенно увеличивается. Не стоит использовать такую систему в точке прохода с большим трафиком (например, на проходной предприятия) – результатом будут очереди перед входом, необходимо будет увеличивать количество точек прохода и дорогостоящих считывателей для обеспечения требуемой пропускной способности системы.

Считыватель

Считыватель подключается к контроллеру и предназначен для извлечения информации от идентификатора пользователя (бесконтактная карта, брелок, отпечаток пальца и т.п.) с последующей передачей данных контроллеру или компьютеру. Обязательными условиями работоспособности системы является:

- совместимость считывателя и выбранного ранее идентификатора;
- одинаковый интерфейс связи между считывателем и контроллером;
- поддержка считывателем записи информации в память носителя кода доступа выбранного типа (например, карты).

Как правило, производители контроллеров систем СКУД также предлагают и ассортимент различных считывателей. Рекомендуется выбирать считыватели от производителя контроллера, что обеспечивает максимальную совместимость оборудования, наличие необходимой технической информации и сервисную поддержку в процессе эксплуатации. При отсутствии в ассортименте считывателей с нужными параметрами произведите поиск и выбор считывателей других производителей.

В точках доступа с большой интенсивностью движения (проходные, входы в здания и т.п.) особенно важно время считывания, то есть время получения информации считывателем от идентификатора.

Для считывателей наружного применения принимается во внимание их климатическое исполнение: температура эксплуатации и показатель пылевлагозащищенности (IPxx). Для снижения риска случайного или умышленного повреждения уличных считывателей рекомендуется использовать врезные вандалозащищенные конструкции. При установке считывателей в помещениях способ их монтажа (накладной, врезной) и дизайн могут быть оговорены заказчиком в ТЗ.

Существуют контроллеры, в корпус которых уже вмонтирован считыватель. В этом случае выбор интерфейса связи контроллер-считыватель не производится. Иногда корпус считывателя может быть оснащен светодиодом для отображения приглашения пользователя к входу в случае успешного считывания кода.

Все более популярными сегодня становятся бесконтактные считыватели, позволяющие дистанционно идентифицировать личность:

- считыватели proximity-меток используют радиочастотную технологию идентификации (RFID) и работают на частоте 125 KHz;

- считыватели смарт-карт используют RFID-технологии, работают на частоте 13,56 MHz и применяются в системах, где требуется более высокий уровень безопасности.

С точки зрения дальности действия обычно рассматриваются:

- бесконтактные считыватели малой дальности - до 10 см;
- бесконтактные считыватели средней дальности - до 1,5 м;
- бесконтактные считыватели высокой дальности действия - от 1,5 м.

Считыватели, не требующие программирования, применяются в СКУД для учета и идентификации пользователя. При появлении LF-карты (жетона, метки) в их зоне действия автоматически считывается серийный номер чипа (UID) или данные из определенного блока памяти карты и передается в компьютер или контроллер.

При выборе высокотехнологичных HF-карт в системе КУД обязательно должен присутствовать программирующий считыватель, поскольку после покупки карты должны пройти перед использованием процедуру подготовки - «предэмиссии». В служебные области smart-карты заносится индивидуальный системный код для защиты от копирования и подделки.

Контроллер

Контроллер - один из основных элементов системы. Он принимает решение о доступе пользователя через контролируемую точку прохода, хранит в своей памяти коды идентификаторов со списком прав каждого из них. Считыватель передает данные идентификатора, они сравниваются контроллером с хранящимися в его памяти кодами, на основании чего принимается решение о возможности прохода и управлении исполнительными устройствами для разблокировки двери, турникета или шлагбаума. Основные параметры контроллеров:

- количество подключаемых считывателей;
- энергонезависимая память идентификаторов;
- энергонезависимая память событий;
- интерфейс связи с сервером (*Ethernet*, *RS-485*);
- количество и тип точек доступа (1дверь / 2 двери / турникет / шлагбаум);
- количество и тип интерфейсов для подключения считывателей.

При выборе моделей контроллеров СКУД необходимо учитывать следующие факторы:

- количество точек доступа в системе;
- количество и тип идентификаторов;
- количество и тип интерфейсов для подключения считывателей;
- интерфейсы связи контроллеров;
- поддержка необходимых режимов доступа;
- поддержка необходимых функций доступа;

- обеспечение интеграции с внешними системами безопасности;
- возможность совместной работы с исполнительными устройствами (замки, турникеты, шлагбаумы, шлюзы и др.);
- поддержка дополнительных подсистем с АРМ: бюро пропусков, проходная, начальник службы безопасности или отдела кадров;
- наличие при необходимости интеграции системы с программами, аналогичными 1С, *Active Directory* и другими.

Необходимо помнить, что количество идентификаторов, поддерживаемых контроллером, должно быть выбрано с запасом. Он необходим для возможности расширения количества персонала или гостевых посетителей.

Интерфейс связи между считывателями и контроллером

Интерфейс предназначен для передачи результата идентификации (считанной с идентификатора информации) со считывателя СКУД на контроллер, который принимает решение о доступе и управляет исполнительными устройствами. В частном случае по интерфейсу может передаваться набранный пользователем на клавиатуре *PIN* код, номер радиобрелка, номер считанной бесконтактной карты, номер шаблона отпечатка пальца и т.д.

Обязательным условием совместной работы считывателя и контроллера является совпадение интерфейсов и протоколов передачи информации.

Доступные интерфейсы для подключения считывателя к контроллеру или к компьютеру: *USB*, *RS-232*, *TCP/IP*; *Wiegand-26*, 34, 37, 40, 42, 56.

Интерфейсы соединения считывателей с контроллером [18-21]:

- *Wiegand*;
- *iButton (Touch Memory, 1-Wire)*;
- *USB*;
- последовательный интерфейсы *RS-232* и *RS-485*;
- *Ethernet*.

Интерфейс *Wiegand*. Популярный интерфейс связи считывателей и контроллера с дальностью до 150-200 метров. Есть варианты реализации *Wiegand*, отличающиеся количеством разрядов в передаваемой информации (26, 34, 37, 40, 42 бит). Вариант указывается с указанием разрядности, например *Wiegand-26* или *Wiegand-34*. Контроллер может поддерживать несколько вариантов.

Интерфейс *iButton* может в описаниях иметь названия *Touch Memory* или *1-Wire*. По двум проводам на идентификаторы *Touch Memory* одновременно подаётся питание и передаются данные. Дальность соединения до 15 метров. Один из часто используемых интерфейсов связи.

Интерфейс *USB*. Используются готовые кабели длиной до 5 метров, а при использовании дополнительных специальных удлинителей возможно создание соединений *USB* длиной 25 метров. Интерфейс *USB* часто используемых для подключения считывателей непосредственно к

компьютеру, на котором производится подготовка идентификаторов для выдачи посетителям.

Последовательный интерфейс RS-232. Обеспечивает двухпроводное подключение контроллера к компьютеру на расстоянии до 5 метров. Из-за малой популярности RS-232 у производителей ПК применяют дополнительные преобразователи RS-232 / USB.

Последовательный интерфейс RS-485. Позволяет передавать данные на расстояние до 1200 метров. Часто используется для объединения контроллеров в сеть (до 32 устройств в одном сегменте). Для подключения к компьютеру дополнительно применяют преобразователи RS-485 / USB;

Интерфейс компьютерной сети Ethernet используется для организации территориально распределенных систем с широкими функциональными возможностями. Для соединения обычно используются кабели UTP и FTP.

Один контроллер доступа может иметь несколько входов для подключения считывателей. Наиболее распространены контроллеры доступа на 1, 2 или 4 считывателя. В зависимости от задачи они могут контролировать доступ через 1-4 точки прохода.

Контроллер в помещении необходимо располагать так, чтобы контролируемые им двери (и считыватель рядом с каждой из них) располагались не дальше максимального расстояния, указанного в документации. Расстояние определяется интерфейсом связи между контроллером и считывателем.

Тип кабеля соединения указан в документации на оборудование. Кроме кабеля для передачи данных могут использоваться провода для реализации различных дополнительных функций: питания считывателя, обеспечения звуковой и световой индикации, передачи данных от контроллера на считыватель при применении идентификаторов с записью в память [24].

Исполнительные устройства

При выборе исполнительного устройства для оборудования точки прохода необходимо учитывать ряд факторов:

- устройство должно соответствовать тому, какой объект преодолевает точку прохода: человек, автомобиль или гужевой транспорт;
- интенсивность движения в точках прохода;
- климатические условия эксплуатации;
- устойчивость к механическим воздействиям для несанкционированного силового преодоления точки доступа;
- особенности конструкции и механическая прочность двери;
- соответствие требованиям дизайна;
- наличие дополнительных функций.

Для дверей внутри помещений используются электромеханические замки и защёлки, а также электромагнитные замки. Электромеханические

замки открываются при подаче электрического питания на короткий промежуток времени (1-3 секунды). Достоинством замка является сохранение закрытого состояния при обесточивании системы и возможность врезной установки, что позволяет оснащать двери системами СКУД при наличии высоких требований по дизайну. К недостаткам можно отнести относительно быстрый износ при интенсивном использовании и слабая защищенность замка от воздействия температуры и воды, что делает невозможным его применение на улице.

Электромеханические замки могут иметь дополнительные функции, связанные с доступом:

- механическая кнопка открывания замка; используется для свободного открывания двери при организации доступа с контролем в одном направлении;
- дополнительный механический ригель; позволяет закрыть замок с использованием механического ключа, при этом открывание его электронной СКУД уже невозможно; используется на объектах с простыми функциями доступа для дополнительной блокировки дверей после ухода последнего сотрудника;
- блокировка замка в открытом состоянии; используется для временного отключения СКУД для удобного перемещения между помещениями, если это допустимо режимом доступа на объекте (например, день открытых дверей в учебном заведении).

Электромеханические защёлки используются там, где есть высокие требования к внешнему виду дверей. К достоинствам можно отнести их широкий ассортимент, который позволяет подобрать нужную модель по цвету, размеру, алгоритму работы, способу монтажа и т.п. Недостатком защёлок является относительная слабая устойчивость к механическим воздействиям.

Электромагнитный замок удерживает дверь в закрытом состоянии за счёт магнитного поля, создаваемого электромагнитной катушкой, по которой течет электрический ток. Основными параметрами замка является усилие удержания, напряжение и сила тока питания замка. К существенным недостаткам можно отнести то, что при пропадании тока замок открывается. Достоинством замков является их высокая надёжность и устойчивость к воздействию воды и температуры. В таблице 16 даны общие рекомендации по выбору рассмотренных устройств [25].

Для проходных и на входах в общественные места могут использоваться турникеты. Турникет имеет тумбу с электромеханическим приводом, съёмные планки и пульт управления для его открытия персоналом охраны. В чрезвычайных ситуациях турникеты в общественных местах не должны задерживать эвакуацию людей, поэтому в таких случаях применяют планки с функцией «антипаника». Турникет может иметь

встроенный считыватель, либо он устанавливается рядом. Для сбора бесконтактных карт могут применяться картоприемники.

Таблица 16 – Применение замков и защёлок для дверей разной конструкции

Материал двери	Электроме- хани- ческая защёлка	Электроме- хани- ческий замок	Электромагнитный замок
Металлопласти- ковые	врезные	врезные	усилие 150-300 кг
Деревянные	накладные / врезные	накладные / врезные	усилие 150-300 кг
Металлические	не используются	накладные / врезные	усилие 300-500 кг
Стеклянные	накладные	накладные	усилие 100-300 кг

Для пропуска автотранспорта используются шлагбаумы и ворота. Шлагбаум состоит из электромеханического привода, стрелы, контроллера и пульта управления. Оборудование, как правило, предлагается поставщиками в виде набора. Для выбора необходимо знать ширину проезда для определения длины стрелы, усилие и интенсивность (частоту) открывания. В качестве аксессуаров используются лампы индикации открытого состояния, активные извещатели обнаружения препятствий для блокировки закрытия стрелы и комплекты радиоканального приёмника с брелками для управления непосредственно из кабины автомобиля

Ворота обладают лучшими свойствами для противодействия несанкционированному доступу. Недостатком их является малая пропускная способность, сложность конструкции, высокая стоимость. В данном курсе ворота подробно не рассматриваются.

Дополнительные элементы СКУД

Для дверей, у которых контроль доступа проводится только в одну сторону (односторонние точки прохода), для беспрепятственного движения пользователя в другую сторону необходимо предусмотреть электрическую кнопку, которая подключается к контроллеру. Получив электрический сигнал от кнопки, контроллер открывает дверь. Также некоторые модели электромеханических замков имеют механическую кнопку для разблокировки двери.

Доводчики являются обязательным атрибутом СКУД для помещений, так как оставленная в открытом состоянии дверь лишает смысла всю систему. Основным параметром при выборе доводчика является усилие, которое необходимо приложить для закрывания двери. Деревянные и металлопластиковые двери имеют меньший вес, чем стеклянные и металлические. Усилие доводчика зависит не только от веса

закрывающей двери, но и от ее размера, так как закрыванию может противодействовать ветровая нагрузка.

По таблице 17 можно определить требуемое усилие закрывания двери в соответствии с Европейскими Нормами *EN1154* и выбрать доводчик для конкретной точки прохода [26].

Таблица 17 – Соответствие требуемого усилия закрывания двери ее параметрам

Усилие закрывания (<i>EN</i>)	Максимальная масса двери (кг)	Максимальная ширина двери (см)
<i>EN 1</i>	20	75
<i>EN 2</i>	40	85
<i>EN 3</i>	60	95
<i>EN 4</i>	80	110
<i>EN 5</i>	100	125
<i>EN 6</i>	120	140
<i>EN 7</i>	160	160

Для дверей выходов на улицу обязательно наличие у доводчика регулировки усилия. Она позволяет компенсировать изменение усилия доводчика в зависимости от температуры, что необходимо для сохранения одинакового усилия открывания двери в тёплое и холодное время года. Цвет доводчика должен гармонировать с цветом двери.

Бесперебойное питание СКУД. Отключение питания систем видеонаблюдения или ОПС приводит к снижению контроля некоторых аспектов безопасности, но не является непосредственной угрозой для человека. Отключение СКУД может привести к блокировке людей в помещениях.

Электромеханические замки или защёлки могут иметь средства механической разблокировки, однако для их активации нужен период времени, в течение которого должно быть организовано электропитание.

После выбора основных элементов системы СКУД необходимо определить параметры питания элементов. Принципы расчета параметров и подбора источников питания аналогичны системам ОПС и видеонаблюдения. При этом необходимо учитывать следующую особенность системы: питание слаботочных элементов (считыватели, контроллеры) и силовых систем (исполнительные устройства) в обязательном порядке ведется от разных источников питания. При срабатывании исполнительных устройств в схеме возникают существенные

электрические импульсы, которые могут вывести слаботочные элементы из строя.

Далее производится расстановка элементов СКУД на плане объекта, выполнение электрических соединений, определение типов и количества проводов.

5.4 Определение элементов интеграции оптико-цифровых систем при проектировании комплексной системы безопасности объекта

При проектировании оптико-цифровых систем безопасности необходимо рассмотреть возможность организации взаимодействия базовых подсистем: ОПС, СОТ и СКУД. Указать способы интеграции подсистем применительно к учебному объекту охраны. Показать элементы взаимодействия, при которых функционирование одной из подсистем зависит от результатов функционирования другой (других) так, что всю совокупность можно рассматривать как единую автоматизированную систему. Основным признаком *интегрированной системы безопасности* (ИСБ) является совместное использование ресурсов подсистем, в результате чего система как целое приобретает качественно новые свойства, в отличие от случая автономной работы подсистем.

В результате проектирования должны быть реализованы и оговорены элементы интеграции подсистем безопасности в соответствии с существующими способами взаимодействия систем.

1. Интеграция всех функций на программно-аппаратном уровне. То есть, все модули системы работают по одному протоколу вне зависимости от того, какую функцию выполняют. Этим достигается максимальная степень взаимосвязи между подсистемами. За счет этого обеспечивается простота и снижение расходов при монтаже и наладке системы. Аппаратное объединение систем реализуется за счет интеграции систем, предусмотренной на этапе разработки оборудования каждой системы, которое может обмениваться информацией и принимать решения самостоятельно, без компьютера управления. Система видеонаблюдения объединяется в комплекс на программном уровне через компьютер управления или с помощью релейных контактов. Это наиболее совершенный тип интегрированных систем. Объединение всех, входящих в ее состав, подсистем происходит за счет общей для них базы данных, программного обеспечения и протокола передачи данных.

2. Интеграция функций на программном уровне предполагает объединение оборудования подсистем безопасности общей программой управления. Оборудование каждой из подсистем работает по своему протоколу. Интеграция подсистем происходит

только за счет программного обеспечения. При этом возможны различные подходы фирм-разработчиков к созданию специализированного ПО. Существуют закрытые программные платформы, которые разрабатываются под собственное оборудование и не позволяют работать с оборудованием других производителей. Более привлекательными и жизнеспособными на рынке систем безопасности рассматриваются открытые программные оболочки с возможностью подключения оборудования различных производителей, которые предоставляют свои программные драйверы для интеграции. Программное обеспечение позволяет конфигурировать, управлять и отображать состояние любого устройства в системе. Существенный недостаток таких систем в том, что при выходе из строя компьютера практически все взаимосвязи между подсистемами нарушаются.

3. Интеграция на аппаратном уровне объединяет все системы безопасности исключительно с помощью аппаратного обеспечения каждой из систем без использования компьютеров управления и внешнего программного обеспечения. Этот способ интеграции реализуется за счет применения имеющихся в составе оборудования программируемых выходных и входных модулей, например, на основе релейных контактов, для передачи информационных сообщений между отдельными системами безопасности. Эти системы строятся на оборудовании разных производителей, а взаимодействие между подсистемами может осуществляться путем включения реле одной подсистемы в шлейф другой. Это наименее эффективные из всех интегрированных систем, поскольку обладают низкой информативностью и лишены возможности реализации сложных алгоритмов взаимодействия между подсистемами.

В состав интегрированной КСБ должны входить не менее двух из проектируемых оптико-цифровых подсистем. Необходимо дать описание информационной, программной и эксплуатационной совместимости технических средств подсистем, входящих в интегрированную систему. В состав технических и программных средств могут входить изделия разных производителей.

ЗАКЛЮЧЕНИЕ

В результате выполнения курсового проекта по созданию комплексной автоматизированной системы безопасности объекта с элементами интеграции формирующих ее оптико-цифровых подсистем студент должен научиться:

- отрабатывать этапы концептуального и рабочего проектирования КСБ;
- владеть методикой выбора варианта охраны объекта и комплекса аппаратно-программных средств обеспечения безопасности в соответствии с требованиями к укреплённости объекта;
- анализировать достоинства и недостатки альтернативных вариантов при выборе программных и аппаратных средств разрабатываемых систем;
- разрабатывать структурные схемы систем с определением принципов действия и установлением технических требований на их отдельные элементы;
- владеть навыками обоснованного выбора основных компонентов проектируемой системы с использованием информационных ресурсов;
- использовать готовые сетевые программные продукты, с целью выявления оптимальных параметров оптико-цифровых КСБ, а также обоснования требований к отдельным звеньям проектируемых подсистем;
- выполнять расчёты необходимых объёмов памяти для хранения данных;
- выполнять технические расчёты по проекту, технико-экономическому анализу системы;
- применять перспективные методы решения профессиональных задач в самостоятельной проектно-конструкторской деятельности.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Влаго Дамьяновски Библия видеонаблюдения — 3, 3-е издание: пер с англ. / Влаго Дамьяновски. – М.: Издательство «Security Focus», 2017. – 422 с.: ил. (Серия «Энциклопедия безопасности») ISBN 978-5-9901176-7-9
- 2 Ворона В.А., Тихонов В.А. Системы контроля и управления доступом – М.: Издательство «Горячая линия Телеком» – 2013. – 272 с.
- 3 Ворона В.А., Тихонов В.А. Технические средства наблюдения в охране объектов – М.: Издательство «Горячая линия Телеком» – 2010. – 184 с. ISBN 978-5-9912-0143-8
- 4 Магауенов Р.Г. Системы охранной сигнализации: основы теории и принципы построения: учебное пособие / Магауенов Р.Г. – 3-е изд. стер. – М.: Издательство «Горячая линия Телеком» – 2017. – 493с. ISBN 978-5-9912-0680-8
- 5 Пескин А.Е. Системы видеонаблюдения. Основы построения, проектирования и эксплуатации. – М.: Издательство «Горячая линия Телеком» – 2013. – 256 с. ISBN 978-5-9912-0336-4
- 6 Синилов В.Г. Системы охранной, пожарной и охранно-пожарной сигнализации: учебник для нач. проф. образования / В.Г. Синилов. — 6-е изд., стер. — М.: Издательский центр «Академия», 2011. — 512 с. ISBN 978-5-7695-8394-0512
- 7 Шанаев Г.Ф., Леус А.В. Системы защиты периметра. – М.: Издательство «Security Focus» – 2011. – 280 с.: цв. ил. ISBN 978-5-9901176-4-8
- 8 Методика выбора ПКП. Информационный портал «Спецавтоматика». Установка сигнализации и видеонаблюдения. Пультовая охрана. URL: - <http://www.specautomatik.ru/index.php/article/244-selection-panel>
- 9 Яновский М. Г. «Как выбрать блок бесперебойного или резервного питания». Информационный портал компании «Бастион». URL: <http://www.bast.ru/articles/stat-yanovsky-vybor>.
- 10 Инструменты проектировщика. Информационный портал компании «Бастион». URL: <https://bast.ru/support/>
- 11 CCTV Information from The CCTV Advisory Service of U.K. URL: <http://www.cctv-information.co.uk>
- 12 Панорамные камеры. Информационный портал компании «AXIS Communications» (Sveden). Производство и проектирование систем видеонаблюдения. URL: <https://www.axis.com/ru/ru/technologies/panoramic-cameras>
- 13 SurroundVideo® Series. Pioneering Multi-Sensor IP Megapixel Cameras. - Информационный портал компании «Arecont Vision, LLC» (USA).

- Производство профессиональных IP камер высокого разрешения. URL: <https://www.arecontvision.com/landing-pages/surround-video/overview.php>
- 14 Panomera® Multifocal Sensor System. - Информационный портал компании «Dallmeier» (Germany). Производство профессиональных систем видеонаблюдения. URL: <https://www.dallmeier.com/en/products/cameras/multifocal-sensor-system-panomerar/models/panomerar-w8-topline.html>
 - 15 PTZ-камеры Axis. Широкий обзор благодаря панорамированию, наклону и зуму. - Информационный портал компании «AXIS Communications» (Sveden). Производство и проектирование систем видеонаблюдения. URL: <https://www.axis.com/ru/ru/products/ptz-cameras>
 - 16 Ручное управление поворотными камерами мышью и клавиатурой TRASSIR PTZ. Информационный портал компании «DSSL» (РФ). Производство цифровых систем видеонаблюдения. URL: <http://www.dssl.ru/products/trassir-ptz>
 - 17 Security Cloud Service. Информационный портал компании ЗАО «РусГард» («RusGuard», РФ) URL: <http://www.rgsec.ru/>, <https://cloud.rgsec.ru>
 - 18 Оборудование ParsecNet. Топология. Информационный портал компании «Нева Электроникс» («NEVA Electronics», РФ). URL: <https://www.parsec.ru/parsecnet3-topology/>
 - 19 СКУД Gate. Информационный портал разработчиков российского брэнда Gate. URL: http://skd-gate.ru/produkty/gate/apparatnaya_chast/
 - 20 SIGUR | Контроллеры. Информационный портал компании «Sigur», РФ. Производитель СКУД. URL: <http://sigursys.com/controllers.php>
 - 21 Контроллеры. Информационный портал компании «PERCo», РФ. Производитель систем безопасности. URL: <https://www.perco.ru/products/kontrollery/>
 - 22 Быков О. MIFARE или Em Marin? Выбираем карту доступа для СКД. Информационный портал компании «NCS», РФ, Производитель ламинированных пластиковых карт, URL: <http://www.neftocard.ru/articles/mifare/vybiraem-kartu-dostupa.php>
 - 23 В чем отличие MIFARE от Em Marin. Информационный портал компании «NCS», РФ, Производитель ламинированных пластиковых карт, URL: <http://www.neftocard.ru/articles/mifare/v-chem-otliche-mifare-ot-emmarin.php>
 - 24 Стасенко Л. Не СКУД-ный выбор. Статьи по безопасности. Информационно-аналитический портал «Мост Безопасности», URL: http://www.security-bridge.com/biblioteka/stati_po_bezopasnosti/ne_skudn_yj_vybor/

- 25 Статьи по тематике контроля доступа HID. Информационный портал «Безопасность доступа» компании «Ландеф», URL: <http://www.idsec.ru/articles.htm>
- 26 CSN EN 1154 Building hardware-Controlled door closing devices-Requirements and test methods - Online European EN Standard Store. URL: <https://www.en-standard.eu/csn-en-1154-building-hardware-controlled-door-closing-devices-requirements-and-test-methods/>

ПРИЛОЖЕНИЕ 1

Пример задания на курсовой проект по дисциплине «Оптико-цифровые системы»

Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ

**“САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ
УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ,
МЕХАНИКИ И ОПТИКИ”**

Факультет: ЛиСИ
Группа: В ХХХХ

Кафедра: ОЭПиС

УТВЕРЖДАЮ
Зав. кафедрой _____
“ ” _____ 20__ г.

ЗАДАНИЕ ПО КУРСОВОМУ ПРОЕКТИРОВАНИЮ

Студентам: Иванову Ивану Ивановичу, Петровой Ольге Петровне, Сидорову Сергею Сергеевичу

Руководитель: Смирнов В.В., Университет ИТМО, доцент
(Фамилия И.О., место работы, должность)

1. Наименование темы Проектирование и исследование комплексной системы безопасности для загородного дома.

2. Срок сдачи студентом законченной работы: 15 декабря 2017 г.

3. Техническое задание

Оптико-цифровые комплексные системы безопасности предназначены для охраны загородного дома, находящегося в коттеджном поселке «Корабельные сосны» (в п. Рощино, Выборгский район Ленинградской области), посредством охранно-пожарной сигнализации, системы охранного телевидения и систем контроля управления доступом.

На территории участка находится дом с 14 помещениями на 3 этажа общей площадью в 546 м². Автономные системы отопления с котлом на первом этаже. Качественная отделка. Гараж на 2 машины в цокольной части дома. В доме 2 входа – основной и запасной через гараж. На третьем этаже дома в кабинете расположен сейф. Отдельные небольшие здания бани и гостевого домика. Баня из 4 помещений общей площадью 45 м². Гостевой дом в 1 этаж, 4 помещения на 70 м². Вход на территорию через калитку и откатные ворота. Дом находится на территории коттеджного поселка. Общая площадь участка составляет 336 м². Категория зданий по взрывопожарной и пожарной опасности Д. На территории присутствует искусственное освещение, включаемое в темное время суток.

Общие технические требования к проектируемой системе безопасности:

Видеонаблюдение периметра, внутренних помещений и территории. Длительность видеозаписей 14 дней, хранить видеоархив на жестком диске. Обеспечить работу

системы охранного телевидения в дневном и ночном режиме. Система охранного телевидения должна решать задачу различения потенциальных нарушителей (крупные черты лица, пол, возраст, для автомобилей – марка, типа кузова). Обеспечить работу системы в течение 12 часов в случае отключения электропитания.

Система охранно-пожарной сигнализации должна контролировать все постройки на территории, сохранять работоспособность в течении 12 часов. Оборудование должно проводить постоянный контроль работоспособности и передавать эту информацию на контрольное устройство. По тревоге сигнал должен передаваться по каналу GSM охране поселка и владельцу дома. Управление системой сигнализации должно быть удобным для неспециалиста.

Система контроля управления доступом должна обеспечивать удобное использование системы владельцем дома, приём посетителей с возможностью диалога с ними с 1-го этажа дома. СКУД позволяет разграничить доступ на территорию дома и гостевого дома, в гараж и в кабинет. Обеспечить работу системы в течение 12 часов в случае отключения электропитания.

4. Содержание пояснительной записки (перечень подлежащих разработке вопросов)

1. Введение.
2. Общая информация об объекте.
3. Основные проектные решения.
4. Монтаж оборудования и электропроводок.
5. Техничко-экономический расчет.
6. Вопросы интеграции подсистем.
7. Заключение.
8. Список использованных источников.

5. Перечень графического материала

1. План объекта
2. Схемы структурные для каждой подсистемы.
3. Схемы расположения оборудования для каждой подсистемы.

6. Исходные материалы и пособия к проекту

1. Рыжова В.А. Проектирование и исследование комплексных систем безопасности. – СПб: НИУ ИТМО, 2013. – 156 с.
2. Андреев А.Л. Автоматизированные видеоинформационные системы - Санкт-Петербург: НИУ ИТМО, 2011. - 120 с.

7. Дата выдачи задания: _____

Руководитель _____
(подпись)

Задание приняли к исполнению _____
(подписи)

ПРИЛОЖЕНИЕ 2

При формировании пояснительной записки и графических материалов в рамках курсового проекта следует руководствоваться следующими стандартами и руководящими документами.

ОБЩАЯ ДОКУМЕНТАЦИЯ

- ГОСТ 7.32-2001 ЕСКД. Отчет о научно-исследовательской работе. Структура и правила оформления.
- ГОСТ 2.105-95 ЕСКД. Общие требования к текстовым документам.
- ГОСТ 7.1-2003 Библиографическая запись. Библиографическое описание. Общие требования и правила составления.
- ГОСТ Р 53704-2009. Системы безопасности комплексные и интегрированные. Общие технические требования
- ГОСТ Р 54906-2012. Системы безопасности комплексные. Экологически ориентированное проектирование. Общие технические требования.
- Постановление Правительства РФ от 16 февраля 2008 г. N 87. О составе разделов проектной документации и требованиях к их содержанию
- Распоряжение Правительства РФ от 3 декабря 2014 г. N 2446-р Об утверждении Концепции построения и развития аппаратно-программного комплекса "Безопасный город"
- ГОСТ 14254-96 (МЭК 529-89) Степени защиты, обеспечиваемые оболочками (КОД IP)
- РД 25.952-90. Системы автоматические пожаротушения, пожарной, охранной и охранно-пожарной сигнализации. Порядок разработки задания на проектирование.
- Федеральный закон от 30 декабря 2009 г. N 384-ФЗ "Технический регламент о безопасности зданий и сооружений"

ДЛЯ ПРОТИВОПОЖАРНЫХ СИСТЕМ

- ГОСТ 12.4.009-83 Система стандартов безопасности труда. Пожарная техника для защиты объектов. Основные виды. Размещение и обслуживание
- ГОСТ 28130-89 (СТ СЭВ 6301-88) Пожарная техника. Огнетушители, установки пожаротушения и пожарной сигнализации. Обозначения условные графические
- ГОСТ 31565-2012 Кабельные изделия. Требования пожарной безопасности
- ГОСТ Р 12.3.047-2012 Система стандартов безопасности труда. Пожарная безопасность технологических процессов. Общие требования. Методы контроля

- Приказ МЧС РФ от 10 июля 2009 г. N 404 "Об утверждении методики определения расчетных величин пожарного риска на производственных объектах"
- Приказ МЧС РФ от 30 июня 2009 г. N 382 "Об утверждении методики определения расчетных величин пожарного риска в зданиях, сооружениях и строениях различных классов функциональной пожарной опасности"
- Решение Совета Евразийской экономической комиссии от 23 июня 2017 г. N 40 "О техническом регламенте Евразийского экономического союза "О требованиях к средствам обеспечения пожарной безопасности и пожаротушения"
- СП 12.13130.2009 Определение категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности
- СП 3.13130.2009. Системы противопожарной защиты. Система оповещения и управления эвакуацией людей при пожаре. Требования пожарной безопасности
- Федеральный закон от 10 июля 2012 г. N 117-ФЗ. О внесении изменений в Федеральный закон Технический регламент о требованиях пожарной безопасности
- Федеральный закон от 22 июля 2008 г. N 123-ФЗ. Технический регламент о требованиях пожарной безопасности

ДЛЯ ОХРАННЫХ СИСТЕМ

- ГОСТ Р 50009-2000 Совместимость технических средств электромагнитная. Технические средства охранной сигнализации. Требования и методы испытаний
- ГОСТ Р 50658-94 (МЭК 839-2-4-90) Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 4. Ультразвуковые доплеровские извещатели для закрытых помещений
- ГОСТ Р 50659-94 (МЭК 60839-2-5:1990) Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации. Раздел 5. Радиоволновые доплеровские извещатели для закрытых помещений
- ГОСТ Р 50775-95 (МЭК 60839-1-11988). Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 1. Общие положения.
- ГОСТ Р 50776-95 (МЭК 60839-1-41989). Системы тревожной сигнализации. Часть 1. Общие требования. Раздел 4. Руководство по проектированию, монтажу и техническому обслуживанию.
- ГОСТ Р 50777-95 (МЭК 60839-2-6:1990) Системы тревожной сигнализации. Часть 2. Требования к системам охранной сигнализации.

Раздел 6. Пассивные оптико-электронные инфракрасные извещатели для закрытых помещений и открытых площадок

- ГОСТ Р 51186-98 Извещатели охранные звуковые пассивные для блокировки остекленных конструкций в закрытых помещениях. Общие технические требования и методы испытаний
- ГОСТ Р 51558-2014 Средства и системы охранные телевизионные. Классификация. Общие технические требования. Методы испытаний
- ГОСТ Р 52435-15 Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний
- ГОСТ Р 52551-2006 Системы охраны и безопасности. Термины и определения
- ГОСТ Р 54830-2011 Системы охраны телевизионные. Компрессия оцифрованных видеоданных. Общие технические требования и методы оценки алгоритмов
- Р 78.36.002-2010 Выбор и применение систем охранных телевизионных
- ГОСТ Р 54831-2011 Системы контроля и управления доступом. Устройства преграждающие управляемые. Общие технические требования. Методы испытаний
- ГОСТ Р 51241-98 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний
- Р 78.36.025-2012 Содержание основных работ по регламентному техническому обслуживанию проводных и радиоканальных СПИ, рекомендованных для применения в подразделениях вневедомственной охраны
- Р 78.36.032-2014 Инженерно-техническая укрепленность и оснащение техническими средствами охраны объектов, квартир и МХИГ, принимаемых под централизованную охрану подразделениями вневедомственной охраны. Часть 2. Квартиры и МХИГ. Методические рекомендации
- Р 78.36.032-2013 Инженерно-техническая укрепленность и оснащение техническими средствами охраны объектов, квартир и МХИГ, принимаемых под централизованную охрану подразделениями вневедомственной охраны. Часть 1.
- РД 78.36.002-2010 Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения
- СП 132.13330.2011 Обеспечение антитеррористической защищенности зданий и сооружений. Общие требования проектирования.

Миссия университета – генерация передовых знаний, внедрение инновационных разработок и подготовка элитных кадров, способных действовать в условиях быстро меняющегося мира и обеспечивать опережающее развитие науки, технологий и других областей для содействия решению актуальных задач.

КАФЕДРА ОПТИКО-ЭЛЕКТРОННЫХ ПРИБОРОВ И СИСТЕМ И ЕЕ НАУЧНО-ПЕДАГОГИЧЕСКАЯ ШКОЛА

Кафедра создавалась в 1937-38 годах и существовала под следующими названиями:

- с 1938 по 1958 год - кафедра военных оптических приборов;
- с 1958 по 1967 год - кафедра специальных оптических приборов;
- с 1967 по 1992 год - кафедра оптико-электронных приборов;
- с 1992 года - кафедра оптико-электронных приборов и систем.

Кафедру возглавляли:

- с 1938 по 1942 год - профессор К.Е. Солодилов;
- с 1942 по 1945 год профессор А.Н. Захарьевский (по совместительству);
- с 1945 по 1946 год - профессор М.А. Резунов;
- с 1947 по 1972 год - профессор С.Т. Цуккерман;
- с 1972 по 1992 год - заслуженный деятель науки и техники РСФСР, профессор Л.Ф. Порфирьев;
- с 1992 по 2007 год - заслуженный деятель науки РФ, профессор Э.Д. Панков.

с 2007 года по настоящее время - почетный работник высшего профессионального образования, профессор В.В. Коротаев.

1938 по 1970 кафедра входила в состав оптического факультета.

В 1970 году кафедра вошла в состав факультета оптико электронного приборостроения, который в 1976 году был переименован в инженерно-физический факультет.

В 1998 г кафедра вошла в состав факультета оптико-информационных систем и технологий.

В 2015 году кафедра вошла в состав факультета лазерной и световой инженерии

Кафедра оптико-электронных приборов и систем (ОЭПиС) осуществляет подготовку профессионалов в области создания оптико-электронных и видеоинформационных приборов и систем, а также в области разработки их программного обеспечения.

Результаты научных исследований кафедры докладываются на ведущих мировых научных форумах, публикуются в виде научных статей и монографий.

Приборы, разработанные на кафедре, поставляются на предприятия России и на предприятия других стран.

Этот уникальный опыт передается нашим студентам.

На кафедре работают 6 докторов наук, профессоров, однако большую часть коллектива составляют молодые люди в возрасте от 18 до 35 лет, в том числе 11 молодых кандидатов наук.

Коллектив кафедры Оптико-электронных приборов и систем (ОЭПиС) – сформировавшаяся научная и научно-педагогическая школа, существующая с 1938 года.

За эти годы были подготовлены более тысячи специалистов, более ста докторов и кандидатов наук.

С 2007 г. заведующим кафедрой является почетный работник высшего профессионального образования Российской Федерации, профессор В.В. Коротаев.

В 2012 году научно-педагогическая школа кафедры ОЭПиС «Оптико-электронное приборостроение» была внесена в реестр ведущих научных и научно-педагогических школ Санкт-Петербурга.

В период с 2016 по 2018 год на кафедре были защищены 11 диссертаций на соискание ученой степени кандидата технических наук.

Подробная информация о кафедре ОЭПиС имеется на сайте кафедры: <http://oep.ifmo.ru/>

Рыжова Виктория Александровна
Горбачев Алексей Александрович
Коротаев Валерий Викторович

Оптико-цифровые системы

Учебное пособие по курсовому проектированию

В авторской редакции

Редакционно-издательский отдел Университета ИТМО

Зав. РИО

Н.Ф. Гусарова

Подписано к печати

Заказ №

Тираж

Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
127101, Санкт-Петербург, Кронверкский пр., 49