Министерство просвещения Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Российский государственный профессионально-педагогический университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

В.В. Мешков, Т.В. Рыжкова

ЛАБОРАТОРНЫЙ ПРАКТИКУМ «КОМПЛЕКСНЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ»

Екатеринбург 2020

Содержание

Лабораторная работа № 1
«Исследование каналов связи RS-232, RS-485»

Цель работы: научиться передавать файлы по каналам связи RS-232, RS-485.

Задачи работы:

1. Настроить каналы связи RS-232, RS-485.
2. Убедиться в работоспособности настроенных каналов связи RS-232, RS-485.
3. Произвести обмен файлами по настроенным каналам связи RS-232, RS-485.
4. Оформить отчет по проделанной работе.

Используемое оборудование: персональный компьютер с предустановленной операционной системой Windows 8, HyperTerminal, кабель RS-232, кабель RS-485.

Теоретические сведения:

Канал передачи данных – это часть коммуникационной сети, состоящая: из технических средств приема и передачи данных, включая линию связи; из средств программного обеспечения и протоколов.

Канал передачи данных определяется наличием минимум двух каналов связи, обеспечивающих передачу сигнала во взаимопротивоположных направлениях.

В зависимости от среды распространения сигнала, для организации каждого из каналов могут быть использованы как одна, так и несколько физических линий связи.

Для обычного случая организации дуплексного канала передачи данных с использование оптических линий связи необходимо использование двух оптических волокон, каждое из которых представляет собой линию связи (часто из состава структурированной кабельной системы).

Для случая организации канала передачи данных с использование кабеля витой пары, необходимо использование всего одного кабеля, пары медных жил которого являются линиями связи каналов связи в составе канала передачи данных.

Интерфейс RS-485 описан в стандартах ANSI EIA/TIA-485-A. Данный интерфейс является наиболее распространенным в промышленной автоматике. В основном данный интерфейс нашел свое широкое применение промышленных сетях (таких как: Modbus, Profibus, DP, ARCNET, BitBus, WorldFip, LON, Interbus и др.). Это связано с тем, что по всем основным показателям данный интерфейс является наилучшим из всех возможных при современном уровне развития технологии. Основными достоинствами интерфейса RS-485 являются:

- двусторонний обмен данными всего по одной витой паре проводов;
- работа с несколькими трансиверами, подключенными к одной и той же линии, т.е. возможность организации сети;
- большая длина линии связи;
- достаточно высокая скорость передачи.

Передача данных осуществляется с помощью дифференциальных сигналов. Разница напряжений между проводниками одной полярности означает логическую единицу, разница другой полярности – ноль.

RS-232 – широко используемый последовательный интерфейс синхронной и асинхронной передачи данных, который в настоящее время используется в самых различных вариантах применения.

При помощи кабеля RS-232 соединяются два устройства, а затем для управления передачи соединенными устройствами используется программное обеспечение – HyperTerminal.

HyperTerminal – терминальная программа, при помощи которой осуществляется доступ к другим компьютерам через нуль-модемный кабель (последовательный порт) или с использованием протокола telnet.

Указания к работе:

Задание 1. Произведите подключение двух персональных компьютеров друг с другом при помощи кабеля RS-232 и произведите операцию по обмену текстовой информацией и текстовым файлом между этими двумя ПК на стеке протоколов TCP/IP.

1.1. Соедините при помощи кабеля RS-232 два персональных компьютера.

1.2. Произведите установку программы HyperTerminal (программа управления передачей данных) на персональный компьютер. В качестве предустановок выполните следующие действия в установленной программе:

1.2.1. В разделе «Параметры подключения» введите код города 343 (код г.Екатеринбург).

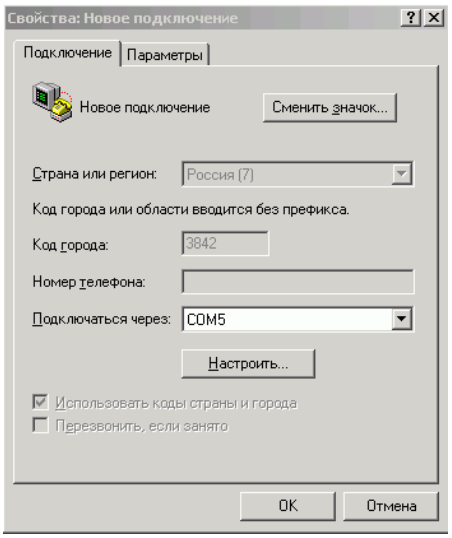

Рисунок 1 – Окно настройки подключения HyperTerminal

1.2.2. В качестве порта подключения выберите COM1.

1.2.3. В разделе параметры порта произведем дополнительные настройки: произведем выбор параметров, с помощью которых можно добиться улучшение производительности подключения, а также повысить скорость передачи данных. Правильный вариант настройки порта приведен на рисунке 2.

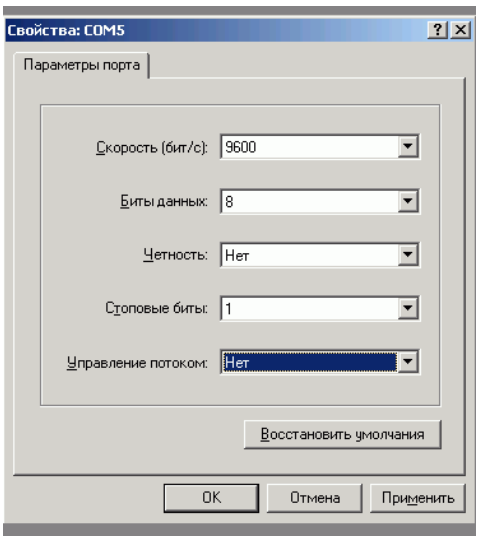

Рисунок 2 – Окно свойств настраиваемого COM-порта

Основными разделами являются:

- **скорость (бит/с).** Базовая единица измерения скорости передачи информации, используемая на физическом уровне сетевой модели OSI или TCP/IP;
- **бит данных.** Был выработан и прижился короткий способ записи параметров UART, таких, как количество бит данных, наличие и тип бита четности, количество стоп-бит. Выглядит как запись вида цифра-буква-цифра, где первая цифра обозначает количество бит данных, например, 8. Буква обозначает наличие и тип бита четности. Встречаются N (No parity) – без бита четности; E (Even parity) – с битом проверки на четность, O (Odd parity) – с битом проверки на нечетность. Последняя цифра обозначает длительность стоп-бита. Встречаются значения 1, 1.5 и 2 для длительности стоп-бита в 1, 1.5 и 2 битовых интервала соответственно. Например, запись 8-N-1 обозначает, что UART настроен на 8 бит данных без бита четности и один стоповый бит. Для полноты параметров эту запись снабжают указанием скорости UART, например, 9600/8-N-1.
- **четность.** Многие реализации UART имеют возможность автоматически контролировать целостность данных методом контроля битовой чётности. Когда эта функция включена, последний бит данных в минимальной посылке («бит чётности») контролируется логикой UART и

содержит информацию о чётности количества единичных бит в этой минимальной посылке. Различают контроль на четность (even), когда сумма количества единичных бит в посылке является четным числом, и контроль на нечетность (odd), когда эта сумма нечетна. При приеме такой посылки UART может автоматически контролировать бит четности и выставлять соответствующие признаки правильного или ошибочного приема;

- **стоповые биты**. Помимо информационных бит, UART автоматически вставляет в поток синхронизирующие метки, так называемые стартовый и стоповый биты. При приёме эти лишние биты удаляются из потока. Обычно стартовый и стоповый биты обрамляют один байт информации (8 бит), при этом младший информационный бит передаётся первым, сразу после стартового. Встречаются реализации UART, передающие по 5, 6, 7, или 9 информационных бит. Обрамленные стартом и стопом биты являются минимальной посылкой. Некоторые реализации UART используют два стоповых бита при передаче для уменьшения вероятности рассинхронизации приёмника и передатчика при плотном трафике. Приёмник игнорирует второй стоповый бит, воспринимая его как короткую паузу на линии;

- **управление потоком**. Ранние устройства с UART могли быть настолько медлительными, что не успевали обрабатывать поток принимаемых данных. Для решения этой проблемы модули UART иногда снабжались отдельными выходами и входами управления потоком. При заполнении входного буфера логика принимающего UART выставляла на соответствующем выходе запрещающий уровень, и передающий UART приостанавливал передачу. Позже управление потоком возложили на коммуникационные протоколы (например, методом XOn/XOff), и надобность в отдельных линиях управления потоком постепенно исчезла.

ПРИМЕЧАНИЕ: если на одном из компьютеров установленные характеристики будут отличаться друг от друга, то сеанс подключения будет нарушен.

1.3. Произведите установку соединения, для этого укажите введите имя пользователя в соответствующее поле и выберите для него соответствующую иконку (иконка может быть и не выбрана, в таком случае она будет принимать общий вид).

1.4. Проверьте установившиеся соединение. Работоспособность подключения можно проверить попробовав набрать несколько символов с клавиатуры, а затем проверить их появление на экране оппонента. В том случае, если данные отобразились на его экране, то можно говорить о том, что подключение состоялось.

1.5. Произведите операцию по обмену файлами (текстовый файл) между двумя клиентами (рабочие станции, подключенные друг к друг при помощи кабеля RS-232).

Задание 2. Произведите подключение двух персональных компьютеров друг с другом при помощи кабеля RS-485 и произведите операцию по обмену текстовой информацией и текстовым файлом между этими двумя ПК.

2.1. Соедините при помощи кабеля RS-485 два персональных компьютера

2.2. Проверьте установившиеся соединение. Установившиеся соединение можно проверить если зайти в пункт подключенные устройства.

2.3. Произведите операцию по обмену файлами (текстовый файл) между двумя клиентами (рабочие станции, подключенные друг к друг при помощи кабеля RS-485).

3. Сформулируйте вывод по проделанной работе и подготовьте отчет по проделанной работе. Отчет должен содержать:

- цель работы;
- задачи работы;
- описание работы;
- ход работ, включая пошаговую фиксацию проделанных действий;
- вывод.

Вопросы для самоконтроля:

1. Что такое канал передачи данных и чем он определяется? Дайте определение понятию.
2. Что такое RS-232, RS-485?
3. Как производится (организуется) обмен информацией (файлами) по стандартам RS-232, RS-485?
4. Назовите основные достоинства стандартов RS-232, RS-485.
5. Что такое стек? На каком стеке протоколов производится операция по обмену информацией, файлами при подключении двух персональных компьютеров с помощью кабеля RS-232.

ОФОРМЛЕННЫЙ ОТЧЕТ НЕОБХОДИМО ВЫЛОЖИТЬ В ИНФОРМАЦИОННЫЙ РЕСУРС ТАЙМЛАЙН В СООТВЕТСТВУЮЩИЙ РАЗДЕЛ ПО ДИСЦИПЛИНЕ

Лабораторная работа № 2
«Системы пожарной сигнализации»

Цель работы: получить теоретические знания и практические навыки по проектированию системы пожарной сигнализации.

Задачи работы:

1. Определить размер помещения.
2. Определить предполагаемые места установки датчиков и иного технического оборудования для реализации заданной системы.
3. Произвести подбор рекомендуемого к установке оборудования.
4. Выполнить описание технических характеристик рекомендуемого к установке оборудования.
5. Построить схему помещения, на котором будет отображено рекомендуемое к установке оборудование.
6. Оценить стоимость спроектированной системы.
7. Оформить отчет по проделанной работе.

Используемое оборудование: персональный компьютер с предустановленной операционной системой Windows 8.

Теоретические сведения:

Основным нормативным документом, который определяет требования в системе охранной сигнализации является – ГОСТ Р 53325-2012 «Технические средства пожарной автоматики».

Пожарная сигнализация (ПС) – это основной элемент в системе безопасности здания, предназначена для выявления пожара на начальной стадии возгорания и выдачи сигнала тревоги.

Автоматическая пожарная сигнализация (АПС) в дополнение к функции обнаружения пожара запускает систему оповещения о пожаре и приводит в действие систему автоматического пожаротушения, систему дымоудаления и другую противопожарную автоматику. Как правило, работа противопожарной

системы более эффективна, если она используется с остальными системами безопасности помещения (охранная сигнализация, видеонаблюдение, система контроля и управления доступом (СКУД) и т. д.). Существуют интегрированные системы охранной и пожарной сигнализации – охранно-пожарная сигнализация (ОПС).

Система пожарной сигнализации состоит из следующих основных компонентов:

Контрольная панель – прибор, который анализирует состояние пожарных датчиков и шлейфов, а также выдаёт команды на запуск пожарной автоматики.

Монитор (панель индикации) или автоматизированное рабочее место (АРМ) – служит для отображения состояния пожарной сигнализации.

Источник бесперебойного питания (ИБП) – служит для обеспечения непрерывной работы сигнализации.

Пожарные датчики (извещатели) – служат для обнаружения возгорания (открытого огня) или продуктов горения (дым, угарный газ и т. д.). По способу обнаружения подразделяются на тепловые, дымовые, датчики пламени и СО. Существуют также мультисенсорные датчики, реагирующие на несколько признаков возгорания.

Исполнительные устройства – это компоненты автоматического пожаротушения или управляемые элементы других систем.

Устройства оповещение – громкоговорители, сирены, системы трансляции. Предназначены для подачи сигнала тревоги.

Дополнительно к датчикам, пожарная сигнализация оснащается ручными пожарными извещателями. Это всем известная «красная кнопка» под стеклом. Устанавливается в легко доступных местах и предназначена для ручной подачи сигнала тревоги.

По способу определения места возгорания системы пожарной сигнализации подразделяются на аналоговые и адресные.

Аналоговые системы определяют место пожара по номеру пожарного шлейфа. На одном шлейфе могут находиться десятки пожарных датчиков. Поэтому, точность определения места пожара низкая. Но для небольших помещений это не важно. Стоимость всех элементов аналоговой сигнализации меньше адресной в разы. Ещё аналоговая система отличается простотой установки.

Адресная пожарная сигнализация указывает на место возникновения пожара. Это современная и высоконадежная система. На крупных объектах это основной тип сигнализаций.

Существует и смешанный тип адресно-аналоговая система пожарной сигнализации. Он применяется при наращивании существующей системы.

По способу опроса пожарных датчиков системы ПС делятся на лучевые и кольцевые. В лучевых схемах пожарной сигнализации опрос происходит по шлейфам, расположенным в форме звезды, центром которой являться пожарная централь. При повреждении шлейфа выявление места обрыва или короткого замыкания затруднено.

Для повышения надежности работы и простоты эксплуатации сейчас все чаще применяется метод опроса по кольцу. Так как опрос одновременно идет с двух сторон это дает возможность работы данной схемы пожарной сигнализации даже с поврежденным в одном месте шлейфом.

Автоматические системы пожаротушения подразделяются на:

- газовые (углекислый газ, азот и др.);
- водяные (тонкодисперсной воды);
- пенные и водопенные (вода с пенообразователем);
- порошковые (специальные порошки);
- аэрозольные.

Системы дымоудаления бывают динамические и статические. Статическая – система отключения вентиляции, предотвращающая проникновение дыма в другие помещения. Динамические системы более эффективны. В них дым удаляется при помощи вытяжной вентиляции.

Вентиляторы работают не только для удаления дыма, но и для подачи свежего воздуха. Для того, чтобы дым не попадал в другие помещения, обычно строят специальные шахты.

Современная автоматическая пожарная сигнализация и система пожаротушения, интегрированная в автоматизированную систему диспетчеризации и управления зданием способна производить мониторинг и оповещение по сотовой связи или Интернет. Правильно спроектированная и построенная, такая система способна эффективно бороться с огнём и задымлением, ликвидировать очаг возгорания ещё до приезда пожарных.

Классификация пожарных извещателей:

1. По способу приведения в действие:

- автоматические;
- ручные.

2. По характеру обмен информацией:

- аналоговые;
- пороговые.

3. По виду контролируемого признака пожара:

- типовые;
- дымовые;
- пламенные;
- газовые;
- комбинированные.

4. По характеру реакции на контролируемый фактор пожара пороговые извещатели пожара подразделяют на:

- максимальные;
- дифференциальные (суммируют за определенное время настроенные характеристики);
- максимально-дифференциальные (могут контролировать как максимальное, так и суммарное значение фактора за время).

5. По агрегатному состоянию контролируемой среды:

- для контроля температуры газообразной среды;
- для контроля температуры жидкой среды и сыпучих тел, посредством внесения в контролируемую среду чувствительного элемента;
- для контроля температуры твердых тел, посредством расположения чувствительного элемента непосредственно на поверхности твердого тела.

6. По принципу действия:
- опто-электронные;
- ионизационные.

7. По конфигурации измерительной зоны:
- тепловые, газовые и дымовые опто-электронные;
- точечные, линейные и многоточечные.

8. По области спектра электромагнитного излучения, воспринимаемого чувствительным элементом:
- ультрафиолетового спектра;
- инфракрасного спектра;
- видимого спектра;
- многодиапазонного спектра.

9. По способу электропитания:
- питаемые по шлейфу;
- питаемые по отдельному проводу;
- питаемые от автономного источника.

10. По возможности установки адреса:
- не адресуемые;
- адресуемые.

11. По числу действий, необходимых для активации:
- активация одним действием;
- активация несколькими действиями.

12. По физической реализации связи с приборами управления:

- радио-канальные;
- проводные;
- оптико-волоконные;
- комбинированные.

Указания к работе:

Примечание: работа выполняется бригадами по 3-4 человека в каждой. Подобранное оборудование у каждой бригады должен различаться, то есть фирмы производители оборудования должны отличаться, при этом требуемое к проектированию оборудование не должно отличаться.

1. На основании выданного преподавателем помещения в качестве объекта для проектирования системы пожарной сигнализации в нем, выполните следующие действия:

- проведите исследование помещения: определите размер помещения (длина, ширина и высота), а также, определите положение аудитории относительно сторон света;
- определите предполагаемые места установки датчиков и иного технического оборудования, согласно их техническим характеристикам и требованиям, предъявляемым к пожарной безопасности в аудитории;
- постройте схему заданного помещения, в которой необходимо отобразить: размер помещения, места установки технического оборудования.

2. Произведите подбор рекомендуемого к установке оборудования для построения модели системы пожарной сигнализации в заданном помещении. Опишите технические характеристики устройств. Определите конечную минимальную стоимость проекта системы пожарной сигнализации в заданном помещении.

3. Сформулируйте вывод по проделанной работе и подготовьте отчет по проделанной работе. Отчет должен содержать:

- цель работы;
- задачи работы;
- описание работы;

- ход работ, включая пошаговую фиксацию проделанных действий;
- вывод.

Вопросы для самоконтроля:

1. Что такое система пожарной сигнализации? Дайте определение понятию.
2. Дайте определение понятию «пожарный извещатель» и приведите их классификацию.
3. Из чего состоит простейшая система автоматической пожарной сигнализации?
4. На какие системы подразделяется автоматические системы пожаротушения?
5. Объясните назначения прибора «контрольная панель» в системе автоматической пожарной сигнализации.

ОФОРМЛЕННЫЙ ОТЧЕТ НЕОБХОДИМО ВЫЛОЖИТЬ В ИНФОРМАЦИОННЫЙ РЕСУРС ТАЙМЛАЙН В СООТВЕТСТВУЮЩИЙ РАЗДЕЛ ПО ДИСЦИПЛИНЕ

Лабораторная работа № 3
«Системы охранной сигнализации»

Цель работы: получить теоретические знания и практические навыки по проектированию системы охранной сигнализации.

Задачи работы:

1. Определить размер помещения.
2. Определить предполагаемые места установки датчиков и иного технического оборудования для реализации заданной системы.
3. Произвести подбор рекомендуемого к установке оборудования.
4. Выполнить описание технических характеристик рекомендуемого к установке оборудования.
5. Построить схему помещения, на котором будет отображено рекомендуемое к установке оборудование.
6. Оформить отчет по проделанной работе.

Используемое оборудование: персональный компьютер с предустановленной операционной системой Windows 8.

Теоретические сведения:

Основным нормативным документом, который определяет требования в системе охранной сигнализации является – ГОСТ Р 50775-95 (МЭК 839-1-1-88). Выдвигаемых требований к системе охранной сигнализации куда больше чем к системе пожарной сигнализации.

Система охранной сигнализации – сложный комплекс технических средств, предназначенный для своевременного обнаружения несанкционированного проникновения в охраняемую зону. Обычно охранная сигнализация интегрируется в комплекс, объединяющий все установленные системы безопасности и инженерные системы зданий, обеспечивающей достоверной адресной информации систем оповещения.

Охранные сигнализации можно разделить на два типа:

1. Автономные системы охранной сигнализации. В автономной системе охранной сигнализации в случае срабатывания активируется система извещения звукового и светового оповещения.

2. Сигнализация с подключением в пункт централизованного наблюдения. Данная сигнализация выводит информацию на удаленный пульт быстрого реагирования.

Контрольная панель – следит за состоянием извещателей (датчики). В случае работы системы (датчиков), подается сигнал на оповещатель.

Современные контрольные панели создаются на базе современных микропроцессорных систем и позволяет подключенные датчики определять в определенные зоны. При попадании объекта в данную зону, может изменяться алгоритм срабатывания системы.

Первый тип зоны – зона входа-выхода, в эту зону включаются охранные датчики, расположенные на пути входа и выхода из помещения. Контрольная панель активирует сигнальные устройства (извещатели), по сигналу от датчиков из этой зоны, только после временной задержки, которая необходима для постановки или снятия системы сигнализации с охраны.

Второй тип зоны – проходная зона, также формирует тревожный сигнал после временной задержки. В эту зону включаются датчики, расположенные по пути движения к пульту управления клавиатуры. Задержка тревоги происходит только в том случае, если порядок полученных сигналов от охранных датчиков соответствует заданному.

Мгновенная зона – при получении контрольной панели и сигнала от датчиков с этой зоны, запуск сигнальный устройств происходит незамедлительно.

24-х часовая круглосуточная зона – если контрольная панель сигнализации получает тревожный сигнал от датчиков из этой зоны, то сигнальные устройства активизируются немедленно, вне зависимости от того, стоит сигнализация на охране или нет. Как правило в эту зону включается тревожная кнопка, применяемая для вызова служб реагирования.

Темперная зона – в эту зону включаются не датчики, а их специальные контакты – тамперы. Тревожный сигнал формируется при попытке демонтажа или скрытия датчиков. Тамперные контакты также могут подключаться от клавиатуры, сирен, и других устройств систем охранной сигнализации.

Устройства управления сигнализацией служат для установки и снятия охранной сигнализации, в том числе и пожарной сигнализации с охраны, используются различные устройства управления:

1. Клавиатуры. Они могут располагаться непосредственно на корпусе контрольной панели или устанавливаться отдельно.
2. Носимый радиобрелок.
3. Электронные ключи. Основное предназначение для доступа к системе.
4. С использованием современных Интернет-технологий.
5. Сигнальные устройства (оповещатели). Устройства, подающие звуковой или световой сигнал в случае отработки контрольной панели при срабатывании датчиков.
6. Звуковые сирены: пьезоэлектрические и динамические. Свето-вспышки являются световыми оповещателями, а тревога посредством переменных ярких вспышек. Комбинированные, включают в себя звуковую сирену и строп-вспышку.
7. Голосовые дозваниватели – при активации передают заранее написанное голосовое сообщение. Передача может осуществляться по проводным телефонным линиям.
8. GSM-модемы. Применяются для передачи тревожных и голосовых СМС сообщений или в качестве каналообразующего оборудования для голосовых дозванивателей.
9. Цифровые коммутаторы – передают информацию о состоянии на объекте охраны на централизованный пульт наблюдения.

Технические средства охранных классификаций – ГОСТ Р 52435-2005. Извещатели классифицируют по следующим признакам функционального назначения:

1. По способу проведения действий:

- автоматические;
- мануальные.

2. По условиям эксплуатации:

- в отапливаемых помещениях;
- в неотапливаемых помещениях (под навесами);
- на открытом воздухе.

3. По виду зоны, контролируемой автоматическими извещателями:

- точечные;
- линейные;
- поверхностные;
- объемные.

4. По физическим принципам, положенным в основу обнаружения:

- электроконтактные;
- магнитоконтактные;
- удароконтактные;
- электромагнитные-бесконтактные;
- пьезоэлектрические;
- емкостные;
- акустические (инфрозвуковые, ультразвуковые);
- вибрационные;
- оптико-электронные (активные и пассивные);
- радио-волновые;
- электростатические;
- трипоэлектрические;
- другие, определяемые новыми разработками.

5. По способу электропитания:

- источники постоянного тока;
- сети переменного тока;
- автономных источников.

6. По сочетанию принципов обнаружения:

- использующие один физический принцип;
- использующие два и более физических принципа;
- комбинированного принципа;
- совмещенные.

Кроме того, все извещатели в системах охраны можно разделить по типу обнаруживаемых тревожных событий, используемые в системах охраны:

1. Датчики движения.
2. Датчики открытия окон, дверей.
3. Датчики разбития стекла.
4. Датчики, реагирующие на приближение и прикосновение.
5. Датчики вибрации.
6. Тревожные кнопки.
7. Комбинированные извещатели:

- Инфракрасный пассивные извещатели. Принцип их работы основан на фиксации изменений теплового излучения, которое возникает в результате, когда человек пересекает чувствительные зоны.
- Инфракрасные активные извещатели. Данные устройства состоят из инфракрасного излучателя и инфракрасного приемника, что позволяет создать рубеж охраны длинной до ста метров.
- Радиоволновые и объемные извещатели. Особенность данных датчиков в особенности их камуфлирования в материально-пропускающие волны. Принцип работы: радиоволновые объемные извещатели формируют сигнал тревоги при регистрации доплеровского сдвига частоты, отраженного СВЧ сигнала, возникающего при движении объекта в электромагнитном поле.

- Линейные радиоволновые извещатели. Срабатывают при пресечении зоны обнаружения. Такие извещатели состоят из передающего и приемного блоков, размещенных в разных концах, размещаемого участка. Принцип работы заключается в анализе амплитудных и временных характеристик принятого сигнала. Используются для обнаружения проникновения в охраняемую зону, а также перемещение объектов в охраняемой зоне. В конструкцию входи блок обработки сигналов, акустический извещатель и акустический приемник.
- Магнитоконтактные извещатели. Данные устройства призваны считывать факт открытия двойных или оконных проемов.
- Акустические охранные извещатели. Используются для обнаружения разбитых стекол и рам.
- Ударно-контактные извещатели: в отличие от акустических, устойчивы и обладают возможностью неразрушающего воздействия на стекло.
- Емкостные охранные извещатели. Данные извещатели фиксируют значения скорость и длительность изменения емкости чувствительного элемента. В качестве чувствительного элемента могут выступать подключенные к извещателю предметы или провода, размещенные на конструктиве охраняемого объекта.
- Вибрационные извещатели. Данные датчики срабатывают при разрушении стен (кирпичных, деревянных, бетонных) и других элементов охраняемой зоны. Принцип работы датчиков основывается на пьезоэлектрическом эффекте, то есть изменения электрического сигнала при вибрации пьезоэлемента.

Указания к работе:

Примечание: работа выполняется бригадами по 3-4 человека в каждой. Подобранное оборудование у каждой бригады должен различаться, то есть фирмы производители оборудования должны отличаться, при этом требуемое к проектированию оборудование не должно отличаться.

1. На основании выданного преподавателем помещения в качестве объекта для проектирования системы охранной сигнализации в нем, выполните следующие действия:

- проведите исследование помещения: определите размер помещения (длина, ширина и высота), а также, определите положение аудитории относительно сторон света;
- определите предполагаемые места установки датчиков и иного технического оборудования, согласно их техническим характеристикам и требованиям, предъявляемым к системе охраны в аудитории;
- постройте схему заданного помещения, в которой необходимо отобразить: размер помещения, места установки технического оборудования.

2. Произведите подбор рекомендуемого к установке оборудования для построения модели системы охранной сигнализации в заданном помещении. Опишите технические характеристики устройств. Определите конечную минимальную стоимость проекта системы охранной сигнализации в заданном помещении.

3. Сформулируйте вывод по проделанной работе и подготовьте отчет по проделанной работе. Отчет должен содержать:

- цель работы;
- задачи работы;
- описание работы;
- ход работ, включая пошаговую фиксацию проделанных действий;
- вывод.

Вопросы для самоконтроля:

1. Дайте определение понятию «система охранной сигнализации».
2. На какие два типа подразделяется система охранной сигнализации? Раскройте содержание функционирования каждого из типов.
3. Какие существуют зоны в системе охранной сигнализации. Раскройте содержание состава устройств и принцип их функционирования в каждой из зон.

4. Для чего предназначены устройства управления сигнализацией?

5. Какие типы извещателей (датчиков) существуют в системе охранной сигнализации?

ОФОРМЛЕННЫЙ ОТЧЕТ НЕОБХОДИМО ВЫЛОЖИТЬ В ИНФОРМАЦИОННЫЙ РЕСУРС ТАЙМЛАЙН В СООТВЕТСТВУЮЩИЙ РАЗДЕЛ ПО ДИСЦИПЛИНЕ

Лабораторная работа № 4
«Системы видеонаблюдения»

Цель работы: научиться записывать видео с камер видеонаблюдения, установленных в учебной аудитории. Разработать схему установку системы видеонаблюдения в заданном помещении.

Задачи работы:

1. С помощью установленной видеокамеры сделать фотографию аудитории.
2. С помощью установленной видеокамеры в аудитории записать короткое видео.
3. Произвести настройки по установке месторасположения сохранения фото-видео-данных с установленных в аудитории камер видеонаблюдения.
4. Разработать модель системы видеонаблюдения в заданном помещении, на основании исследования помещения, определения его площади.
5. Определить места установки и необходимое количество видеокамер, для реализации комплексного видеонаблюдения в помещении.
6. Осуществить подбор оборудования, для разработанной модели системы видеонаблюдения.
7. Оформить отчет по проделанной работе.

Используемое оборудование: персональный компьютер с предустановленной операционной системой Windows, камеры видеонаблюдения – 2шт «TrendNet TV-IP572P».

Теоретические сведения:

Система видеонаблюдения и контроля – система замкнутого телевидения или система охранного телевидения, предназначенная для

организации видеонаблюдения на ответственных объектах. Основные задачи системы видеонаблюдения;

- текущее наблюдение;
- работа с архивом видеозаписей;
- дистанционный просмотр текущего изображения и архива;
- запись видеоизображения по движению или срабатывание охранных датчиков;
- интеграция с системой охранной и пожарной сигнализации (в особых случаях);
- интеграция с аппаратно-программным комплексом с системой контроля;
- масштабируемость и модернизация системы видеонаблюдения при необходимости;
- текущее наблюдение и управление всей системой из одной точки, в том числе организация видеонаблюдения через интернет.

Данные системы представляют собой сложный технический комплекс, состоящий из:

- видеокамер;
- мониторов;
- регистраторов;

Обмен информацией между устройствами, входящими в состав автоматизированных систем (компьютерами, контроллерами, датчиками, исполнительными устройствами) происходит в общем случае через информационную сеть, требования к которой находятся на уровне промышленных сетей. Данные сети отличаются от офисных тем, что обладают следующими свойствами:

- специальным конструктивным исполнением, обеспечивающим защиту от внешних факторов;
- температурным диапазоном;

- повышенная устойчивость к воздействию электро-магнитных помех;
- возможность резервирования для повышения надежности;
- повышенная надежность передачи данных;
- возможность к самовосстановлению после сбоя;
- повышенная прочность у кабеля, изоляция, разъемов, элементов крепления;
- повышенная надежность передачи данных;
- детерминированность (определенностью) времени доставки сообщений;
- возможность работать в реальном режиме времени (с малой постоянной и известной величиной задержки);
- работа с длинными линиями связи.

В настоящий момент насчитывается около 50 типов промышленных сетей, которые в настоящий момент завоевывают соответствующие системы.

Информационной сетью называется комплекс оборудования и программного обеспечения, который обеспечивает информационный обмен (коммуникации). Информационная сеть является основой для построения распределенной системы сбора данных и их управления. Для соединения сети с ее компонентами, устройствами, узлами сети, выполняется с помощью интерфейса. Сетевым интерфейсом называют логическую или физическую границу, между устройствами и средой передачи информации. Обычно этой границей является набор электронных компонентов и связанного с ним программного обеспечения. При существенных модификациях внутренней структуры устройства или программного обеспечения. Интерфейс остается без изменений. Наиболее важными параметрами интерфейса является пропускная способность и максимальная длинна подключенного кабеля.

Промышленные интерфейсы обычно обеспечивают гальваническую развязку, между соединяемыми устройствами. Наиболее распространены следующие интерфейсы. Взаимодействующие устройства для обмена

информацией должны иметь одинаковый протокол обмена. В простейшей форме протокол – набор правил, который управляет обменом информацией. Он определяет синтаксис и семантику сообщений, операций управления, синхронизацию, и состояние при коммуникации. Протокол может быть реализован аппаратно, программно, или программно-аппаратно. Обычно сеть использует несколько протоколов, образующих сеть стек-протоколов – набор, связанных коммуникационных протоколов, которые функционирую совместно и используют некоторые или все семи уровней модели OSI.

1. К числу основных признаков классификации относится:

1.1. Место расположения системы.

1.2. Принципы управления.

1.3. Уровень интеллекта.

1.4. Способ передачи сигналов.

1.5. Тип используемых видеокамер.

1.6. Число используемых видеокамер.

1.7. Разрешение видеокамер и др.

2. По типу использования оборудования:

2.1. Аналоговые системы наблюдения. Преимущества аналоговых систем видеонаблюдения заключаются в невысокой стоимости оборудования, высокой надежности, простоте конструкций и эксплуатаций, что позволяет использовать их персонал невысокой квалификации. Недостатком считается, необходимость постоянного обслуживания видео-носителей (видеомагнитофона).

2.2. Цифровые системы видеонаблюдения. Преимущества таких систем, большие объемы записи информации, простота поиска информации, возможность интеграции с другими системами и интернетом, применение дешевого видеоархива, использование стандартных типов соединения (подключения), возможность передачи данных через wi-fi. Основными недостатками считается, относительно высокая стоимость оборудования, требование специализированного персонала.

3. По типу установки:

3.1. Системы наружного видеонаблюдения, предназначенные для наблюдения по периметру здания).

3.2. Системы внутреннего видеонаблюдения, предназначенные для контроля объекта.

3.3. Системы скрытого наблюдения, предназначенные для ведения скрытой съемки.

4. По месту нахождения:

4.1. Стационарные системы.

4.2. Мобильные системы.

5. По уровню интеллекта:

5.1. Системы с низким уровнем интеллекта, предназначенные в основном для записи информации.

5.2. Системы с высоким уровнем интеллекта, предназначенные для выполнения функции распознания обстановки, изменение объектов и др.

6. По способу передачи:

6.1. Проводные системы

6.2. Оптоволокно.

7. По типу видеокамер, используемых в системе:

7.1. Камеры черно-белой съемки, которые характеризуются низкой стоимостью, высокой разрешающей способностью (по сравнению с цветными в 1.5-2 раза) и высокой чувствительностью (в 4-8 раз, по сравнению с цветными).

7.2. Цветные камеры, которые характеризуются более лучшей идентификацией за наблюдаемым объектом.

8. По числу использования видеокамер в системе:

8.1. Простые системы (от одной камеры до десятка).

8.2. Сложные системы (до нескольких десятков).

Разрешение видеокамер: оценивается по количеству линий, которая может зафиксировать видеокамера (обычная 380*420, высокое разрешение 580*420)

Комплектация системы видеонаблюдения зависит от требований, предъявляемых безопасности объекта.

Как правило, минимальная конфигурация системы видеонаблюдения включает:

- видеокамеры;
- устройство отображения видеоинформации (монитор);
- устройство обработки видеосигналов;
- видео коммутаторы;
- видео-мультиплексоры;
- видеодетекторы движения и др.;
- записывающие устройства (видеомагнитофоны и регистраторы);
- каналы устройства передачи видеосигналов.

В крупные системы видеонаблюдения, могут быть включены дополнительные управляющие и вспомогательные устройства (усилители-распределители, модуляторы, телеметрические приемники, матричные коммутаторы, поворотные устройства для видеокамер, видео принтеры и др. Система скрытого видеонаблюдения

Эффективность охраны того или иного объекта, существенно возрастает, при использовании системы скрытого наблюдения. Технической базой для организации служат видеокамеры на основе матрицы ЦЗС, что позволяет снизить габаритные размеры и увеличить надежность видеосистемы. Важным преимуществом таких видеокамер является их высокая чувствительность в инфракрасном диапазоне, это позволяет обеспечить качественную съемку даже в условиях полной темноты используя инфракрасную подсветку. Значительным плюсом такой съемки является то, что нарушитель в большинстве случаев не предполагает самой возможности наблюдения и съемки в темноте. К типовым заданиям, предъявляемым

установленным системам, различного профиля, является предотвращение кражи со стороны персонала. Основной частью систем скрытого видеонаблюдения является масштабируемость своего условия.

К основным характеристикам камер видеонаблюдения относятся:

- фокус и цвет чувствительности объектива;
- разрешающая способность;
- формат ПЗС матрицы;
- возможность цифровой обработки сигнала;
- угол обзора видеокамеры.

Все эти характеристики тесно взаимосвязаны между собой. И определяют возможности видеокамер. Основным показателем при расчете размещения и выборе видеокамер является угол обзора видеокамеры.

Угол обзора характеризует видимый обхват наблюдаемого пространства, напрямую зависит от фокусного расстояния объекта и размера ПЗС матрицы. Так при одинаковых объектах угол обзора будет больше у видеокамеры с большей матрицей. Угол обзора важный параметр для камеры наблюдения, чем он больше, тем шире зона наблюдения. Отсюда следует что при большом охвате наблюдения одной камерой их меньше понадобиться для контроля над определенной площадью, и для определения количества приборов наблюдения необходимо иметь угол обзора.

Расчет фокуса можно производить несколькими методами, угол обзора напрямую зависит от фокусного расстояния:

$$f = \frac{r * a}{l}$$

f – фокусное расстояние объектива

r – расстояние до объекта

a – размер стороны матрицы (применяется та сторона, которая определяет плоскость наблюдения)

l – размеры объекта в метрах

h – размер объекта на экране монитора

Таким образом, будет осуществлен расчет при котором объект будет занимать почти весь экран монитор, принимая во внимание важность объекта и целесообразность наблюдения территории, находящейся вокруг него, определяется в процентах та часть экрана, которую может занимать охраняемый объект. Для учета процентного соотношения

$$f = \frac{r * a}{(100 * \frac{l}{h})}$$

Объект наблюдения – въездные ворота на территорию предприятия, задача, стоящая перед системой наблюдения – фиксировать марки и номерные знаки, въезжающих и выезжающих автомобилей. Для расчета имеются данные r=10 м, расстояние от объектива до границы ворот. h – 5%, размер объекта на мониторе по горизонтали. Размер матрицы a=8,46 мм. Реальный размер который мы должны распознать 0,52 мм номерного знака.

	8, мм						
	2	4	6	8	12	16	50
	Угол альфа в градусах						
¼	64	48	33	25	17	13	4
⅓	78	59	42	32	22	16	5
½	94	74	54	42	28	21	6

Угол обзора можно определить более коротким путем, но необходимо учесть, что недорогие объективы имеют оптические искажения, особенно сильна сферическая аберрация

$$A=\propto= 2arctg(\frac{b}{2s})$$

Современные фокусные объективы позволяют достичь угла свыше 182 градусов. Возникает проблема, такая как линейное начертании объектов, сильно искажаются в сферической аберрации или изображения принимают изогнутую форму, отсюда следует, что тем больше фокусное расстояние, тем четче виден объект, но под меньшим углом наблюдения. Для расчета нам необходима такая характеристика как четкость изображения.

Четкость изображения или разрешение камер наблюдения – способность устройства четко фиксировать минимальные размеры объекта наблюдения, на определенном расстоянии до камер. Разрешение и соответственно четкость

изображения, зависит от качества объектива и его фокусного расстояния, и от технических характеристик ПЗС (прибор зарядной связи) матрицы, а также от расстояния от объектива до реального объекта.

Если используется визуальное приемное устройства монитор, то добавляется:

1. Качество преобразования видеосигнала в приемном устройстве.
2. Технические характеристики воспроизводящего устройства монитора.

Для того, чтобы увеличить разрешение (детализацию) объекта, необходимо объект приблизить к объективу.

Фокусное расстояние объектива, мм	Горизонтальный угол обзора для матрицы в одну треть дюйма, градус	Возможность обнаружения человека, м	Возможность идентификации человека, м	Возможность определения номера автомобиля,
2,8	86	19	1,4	-
3,6	72	25	1,8	-
4,0	67	28	2	5
8,0	36	56	4	5
12,0	25	84	6	8
25,0	12	175	12,5	16
50,0	6	350	25	33
80,0	3,3	560	40	53
120,0	2,1	840	60	80

При расчетах дистанций, за основу могут применяться европейские нормы:

1. 20 пикселей на метр – норма для разрешения при обнаружении объекта в поле обзора.
2. 100 пикселей на метр – показатель применяемый при распознавании объектов.
3. 250 пикселей на метр – показатель применяемый при идентификации объектов.

Кроме факторов, влияющих на угол обзора, в процессе эксплуатации возникают такие факторы, влияющие на показатели видеокамер:

- нарушение работоспособности объектива;
- некачественное закрепление корпуса к опорной конструкции;

- утрата свойств смазочной составляющей;
- электронные помехи.

Кроме теоретических просчетов по углу обзора важными факторами являются:

- точка установки должна обеспечить максимальный обзор в вертикальных и горизонтальных плоскостях;
- защищенность от воздействия климатических или каких-либо механических воздействий;
- защищенность от воздействий посторонних лиц;
- доступность при совершении профилактических работ;

Каждый объект требует индивидуального подхода при организации системы видеонаблюдения.

Комплексное применение камер видеонаблюдения в системе обеспечения безопасности и контроля в аудитории, призвано обеспечить:

- мониторинг безопасности учащихся и педагогического коллектива;
- повышение уровня дисциплины и снижение уровня повреждений имуществу учреждения;
- решение спорных моментов на контрольных и экзаменах;
- предупреждение чрезвычайных ситуаций будь то ситуации техногенного характера, либо преступные действия злоумышленников.

Указания к работе:

Примечание: работа выполняется бригадами по 3-4 человека в каждой. Подобранное оборудование у каждой бригады должен различаться, то есть фирмы производители оборудования должны отличаться, при этом требуемое к проектированию оборудование не должно отличаться.

1.1. Определите тип и модель установленной в аудитории камеры видеонаблюдения. Составить характеристику на установленные в аудитории камеры видеонаблюдения.

1.2. Определите угол обзора камер и наличие слепых зон при ведении видеонаблюдения в аудитории. На основании полученных результатов составьте схему, в состав которой должен быть включен примерный угол обзора камер видеонаблюдения (в качестве доказательства используется формула по расчету угла обзора для камер видеонаблюдения) с учетом месторасположения камер, а также отражение возможных слепых зон. Сформулируйте вывод об эффективности ведения видеонаблюдения у учебной аудитории.

1.3. Произведите настройку камер видеонаблюдения: работа по подключению к управлению видеокамерами, работа по выбору месторасположения для сохранения потока фото-видео-данных по умолчанию. После проведения настроек, сделайте несколько снимков с разных камер учебной аудитории, а также произведите запись короткого видео с одной из установленных камер.

2.1. На основании выданного преподавателем помещения в качестве объекта для составления модели системы видеонаблюдения в нем, выполните следующие действия:

- проведите исследование помещения: определите размер помещения (длина, ширина и высота), определите загруженность помещения во время нахождения в нем людей и примерную проходимость количества людей за день, определите требования, которые предъявляются к системе видеонаблюдения в данном помещении.
- на основании полученных данных определите места установки камер видеонаблюдения (с учетом угла обзора и эффективности расположения камер), их минимальное количество для осуществления комплексного видеонаблюдение за всей областью помещения, а также возможности осуществления видеокамерами прикрытия друг друга. Требование, предъявляемое к системе видеонаблюдения – возможность четкого считывания лиц, входящих в помещение.

- постройте схему выданного помещения, в которой необходимо отобразить: размер помещения, места установки камер и их угол обзора (в качестве доказательства используется формула по расчету угла обзора для камер видеонаблюдения).

2.2. Произведите подбор необходимого оборудования для построенной модели системы видеонаблюдения в заданном помещении. Опишите технические характеристики устройств. Определите конечную минимальную стоимость проекта системы видеонаблюдения в заданном помещении.

3. Сформулируйте вывод по проделанной работе и подготовьте отчет по проделанной работе. Отчет должен содержать:

- цель работы;
- задачи работы;
- описание работы;
- ход работ, включая пошаговую фиксацию проделанных действий;
- вывод.

Вопросы для самоконтроля:

1. Дайте определение понятию система видеонаблюдения. В чем заключаются основные задачи данной системы?
2. Какой минимальный набор технического оборудования необходим для реализации системы видеонаблюдения и контроля?
3. Как происходит обмен между устройствами, входящими в состав автоматизированных систем? Какими свойствами обладает данная сеть?
4. Назовите основные признаки классификации системы видеонаблюдения и контроля.
5. Какие системы наблюдения используются на данный момент? Приведите их виды и дайте характеристику каждому из них.
6. Какие характеристики относят к основным характеристикам камер видеонаблюдения?
7. Как произвести расчет фокуса для камеры видеонаблюдения?

8. Какие факторы напрямую влияют на показатели видеокамер в процессе их эксплуатации? Приведите примеры.

9. Чем характеризуется комплексное использование камер видеонаблюдения в системе обеспечения безопасности и контроля в учебных аудиториях? Приведите примеры.

ОФОРМЛЕННЫЙ ОТЧЕТ НЕОБХОДИМО ВЫЛОЖИТЬ В ИНФОРМАЦИОННЫЙ РЕСУРС ТАЙМЛАЙН В СООТВЕТСТВУЮЩИЙ РАЗДЕЛ ПО ДИСЦИПЛИНЕ

Лабораторная работа № 5
«Системы контроля и управления доступом»

Цель работы: получить теоретические знания и практические навыки по проектированию системы контроля и управления доступом.

Задачи работы:

1. Произвести настройку систему контроля и управления доступом в заданном помещении.
2. Осуществить настройку приборов контроля и управления доступом.
3. Проверить работоспособность настроенной системы.
4. Оформить отчет по проделанной работе.

Используемое оборудование: …

Теоретические сведения:

Система контроля и управления доступом (СКУД) – совокупность программно-аппаратных технических средств безопасности, имеющих целью ограничение и регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через «точки прохода»: двери, ворота, КПП.

Основная задача – управление доступом на заданную территорию (кого пускать, в какое время и на какую территорию), включая также ограничение доступа на заданную территорию идентификация лица, имеющего доступ на заданную территорию.

Дополнительные задачи:

- учёт рабочего времени;
- расчет заработной платы (при интеграции с системами бухгалтерского учёта);
- ведение базы персонала / посетителей;
- интеграция с системой безопасности, например: с системой видеонаблюдения для совмещения архивов событий систем, передачи системе

видеонаблюдения извещений о необходимости стартовать запись, повернуть камеру для записи последствий зафиксированного подозрительного события; с системой охранной сигнализации (СОС), например, для ограничения доступа в помещения, стоящие на охране, или для автоматического снятия и постановки помещений на охрану; с системой пожарной сигнализации (СПС) для получения информации о состоянии пожарных извещателей, автоматического разблокирования эвакуационных выходов и закрывания противопожарных дверей в случае пожарной тревоги.

На особо ответственных объектах сеть устройств СКУД выполняется физически несвязанной с другими информационными сетями.

Используемое оборудование при проектировании системы контроля и управления доступом:

1. Преграждающие устройства:

1.1. Устанавливающиеся на двери:

1.1.1. Электрозащёлки – наименее защищены от взлома, поэтому их обычно устанавливают на внутренние двери. Электрозащёлки, как и другие типы замков, бывают открываемые напряжением (то есть дверь открывается при подаче напряжения питания на замок), и закрываемые напряжением (открываются, как только с них снимается напряжение питания, поэтому рекомендованы для использования пожарной инспекцией).

1.1.2. Электромагнитные замки – практически все запираются напряжением, то есть пригодны для установки на путях эвакуации при пожаре.

1.1.3. Электромеханические замки – достаточно устойчивы ко взлому (если замок прочный механически), многие имеют механический перевзвод (это значит, что если на замок подали открывающий импульс, он будет разблокирован до тех пор, пока дверь не откроют).

1.2. Устанавливающиеся на проходах/проездах:

1.2.1. Турникеты – используются на проходных предприятий, общественно значимых объектах (стадионы, вокзалы, метро, некоторые госучреждения) – везде, где требуется организовать контролируемый проход

большого количества людей. Турникеты делятся на два основных типа: поясные и полноростовые. Если рядом с турникетом нет быстро открывающегося свободного прохода (на случай пожара), поясной турникет должен быть оборудован т.н. планками «антипаника» – планками, переламывающимися усилием нормального человека (требование пожарной инспекции).

1.2.2. Шлюзовые кабины – используются в банках, на режимных объектах (на предприятиях с повышенными требованиями к безопасности).

1.2.3. Ворота и шлагбаумы – в основном, устанавливаются на въездах на территорию предприятия, на автомобильных парковках и автостоянках, на въездах на придомовую территорию, во дворы жилых зданий. Основное требование – устойчивость к климатическим условиям и возможность автоматизированного управления (при помощи системы контроля доступа). Когда речь идёт об организации контроля доступа проезда, к системе предъявляются дополнительные требования – повышенная дальность считывания меток, распознавание автомобильных номеров (в случае интеграции с системой видеонаблюдения).

1.2.4. Автоматические дорожные барьеры – используются для гарантированного предотвращения несанкционированного проезда автотранспорта на защищаемую территорию. Являются мерами антитеррористической защиты, поскольку проезд через поднятый барьер приводит к разрушению подвески автомобиля.

2. Идентификатор. Основные типы исполнения – карточка, брелок, метка. Является базовым элементом системы контроля доступа, поскольку хранит код, который служит для определения прав («идентификации») владельца. Это может быть Touch memory, бесконтактная карта (например, RFID-метка), или устаревающий тип карт с магнитной полосой. В качестве идентификатора может выступать так же код, вводимый на клавиатуре, а также отдельные биометрические признаки человека – отпечаток пальца,

рисунок сетчатки или радужной оболочки глаза, трехмерное изображение лица.

Надежность (устойчивость к взлому) системы контроля доступа в значительной степени определяется типом используемого идентификатора: например, наиболее распространенные бесконтактные карты proximity могут подделываться в мастерских по изготовлению ключей на оборудовании, имеющемся в свободной продаже. Поэтому для объектов, требующих более высокого уровня защиты, подобные идентификаторы не подходят. Принципиально более высокий уровень защищенности обеспечивают RFID-метки, в которых код карты хранится в защищённой области и шифруется.

Кроме непосредственного использования в системах контроля доступа, RFID-метки широко применяются и в других областях. Например, в локальных расчетных системах (оплата обедов в столовой и других услуг), системах лояльности и так далее.

3. Автономный контроллер – это «мозг» системы: именно контроллер определяет, пропустить или нет владельца идентификатора в дверь, поскольку хранит коды идентификаторов со списком прав доступа каждого из них в собственной энергонезависимой памяти. Когда человек предъявляет (подносит к считывающему устройству) идентификатор, считанный из него код сравнивается с хранящимся в базе, на основании чего принимается решение об открытии двери.

Сетевой контроллер объединяется в единую систему с другими контроллерами и компьютером для возможности централизованного контроля и управления. В таком случае решение о предоставлении доступа может приниматься как контроллером, так и программным обеспечением головного компьютера. Чаще всего объединение контроллеров в сеть осуществляется посредством промышленного интерфейса RS-485 или локальной сети Ethernet.

В случаях, когда необходимо обеспечить работу контроллера при авариях электросети, блок контроллера обеспечивается собственным

аккумулятором, либо внешним блоком резервного питания. Время работы от аккумулятора может составлять от нескольких часов до нескольких суток.

4. Считыватель – Это устройство, которое получает («считывает») код идентификатора и передает его в контроллер. Варианты исполнения считывателя зависят от типа идентификатора: для «таблетки» – это два электрических контакта (в виде «лузы»), для proximity-карты – это электронная плата с антенной в корпусе, а для считывания, например, рисунка радужной оболочки глаза в состав считывателя должна входить камера. Если считыватель устанавливается на улице (ворота, наружная дверь здания, проезд на территорию автостоянки), то он должен выдерживать климатические нагрузки – перепады температур, осадки – особенно, если речь идет об объектах в районах с суровыми климатическими условиями. А если существует угроза вандализма, необходима ещё и механическая прочность (стальной корпус). Отдельно можно выделить считыватели для дальней идентификации объектов (с расстоянием идентификации до 50 м.). Такие системы удобны на автомобильных проездах, парковках, на въездах на платные дороги и т. п. Идентификаторы (метки) для таких считывателей, как правило, активные (содержат встроенную батарейку).

5. Конвертор среды. Служат для подключения аппаратных модулей СКУД друг к другу и к ПК. Например, являются популярными конверторы RS-485 ↔ RS-232 и RS-485 ↔ Ethernet. Некоторые контроллеры СКУД уже имеют встроенный интерфейс Ethernet, позволяющий без использования каких-либо дополнительных устройств подключаться к ПК и связываться друг с другом.

6. Вспомогательное оборудование. Блоки бесперебойного питания, дверные доводчики, датчики открывания двери, кнопки, провода, видеонаблюдение и т. д.

7. Программное обеспечение. Не является обязательным элементом системы контроля доступа, используется в случае, когда требуется обработка информации о проходах, построение отчетов, либо когда для начального программирования, управления и сбора информации в процессе работы

системы необходимо сетевое программное обеспечение, устанавливаемое на один или несколько ПК, соединенных в сеть. Все СКУД можно отнести к двум большим классам или категориям: сетевые системы и автономные системы.

Виды используемых систем при проектировании систем контроля и управления доступом:

8. Сетевые системы. В сетевой системе все контроллеры соединены с компьютером, что дает множество преимуществ для крупных предприятий, но совсем не требуется для «однодверной» СКУД. Сетевые системы удобны для больших объектов (офисы, производственные предприятия), поскольку управлять даже десятком дверей, на которых установлены автономные системы, становится чрезвычайно трудно. Незаменимы сетевые системы в следующих случаях:

- если необходимо реализовать сложные алгоритмы допуска групп сотрудников с разными привилегиями в разные зоны предприятия и иметь возможность оперативно их изменять;
- если необходимо выборочно удалять или создавать пропуска (метки) для большого количества точек прохода или для большого количества сотрудников (большая текучка и утери пропусков);
- если необходима информация о произошедших ранее событиях (архив событий) либо требуется дополнительный контроль в реальном времени. Например, в сетевой системе существует функция фотоверификации: на проходной при поднесении входящим человеком идентификатора к считывателю, служащий (вахтер, охранник) может на экране монитора видеть фотографию человека, которому в базе данных присвоен данный идентификатор, и сравнить с внешностью проходящего, что подстраховывает от передачи карточек другим людям;
- если необходимо организовать учёт рабочего времени и контроль трудовой дисциплины;

- если необходимо обеспечить взаимодействие (интеграцию) с другими подсистемами безопасности, например, видеонаблюдением или пожарной сигнализацией).

В сетевой системе из одного места можно не только контролировать события на всей охраняемой территории, но и централизованно управлять правами пользователей, вести базу данных. Сетевые системы позволяют организовать несколько рабочих мест, разделив функции управления между разными сотрудниками и службами предприятия.

В сетевых системах контроля доступа могут применяться беспроводные технологии, так называемые радиоканалы. Использование беспроводных сетей зачастую определяется конкретными ситуациями: сложно или невозможно проложить проводные коммуникации между объектами, сокращение финансовых затрат на монтаж точки прохода и т. д. Существует большое количество вариантов радиоканалов, однако в СКУД используются только некоторые из них:

- Bluetooth. Данный вид беспроводного устройства передачи данных представляет собой аналог Ethernet. Его особенность заключается в том, что отпадает необходимость прокладывать параллельные коммуникации для объединения компонентов при использовании интерфейса RS-485.
- Wi-Fi. Основное преимущество данного радиоканала заключается в большой дальности связи, способной достигать нескольких сотен метров. Это особенно необходимо для соединения между собой объектов на больших расстояниях (?). При этом сокращаются как временные, так и финансовые затраты на прокладку уличных коммуникаций.
- ZigBee. Изначально сферой применения данного радиоканала была система охранной и пожарной сигнализации. Технологии не стоят на месте и активно развиваются, поэтому ZigBee может использоваться и в системах контроля доступа. Данная беспроводная технология работает в нелицензируемом диапазоне 2,45 ГГц.

- GSM. Преимущество использования данного беспроводного канала связи — практически сплошное покрытие. К основным методам передачи информации в рассматриваемой сети относятся GPRS,SMS и голосовой канал.

- Нередки ситуации, когда установка полноценной системы безопасности может оказаться неоправданно дорогой для решения поставленной задачи. В таких ситуациях оптимальным решением будет установка автономного контроллера на каждую из точек прохода, которые необходимо оборудовать доступом.

9. Автономные системы. Автономные системы дешевле, проще в эксплуатации, не требуют прокладки сотен метров кабеля, использования устройств сопряжения с компьютером, самого компьютера. При этом к минусам таких систем относится невозможность создавать отчеты, вести учёт рабочего времени, передавать и обобщать информацию о событиях, управляться дистанционно. При выборе автономной системы с высокими требованиями по безопасности рекомендуется обратить внимание на следующее:

- Считыватель должен быть отделен от контроллера, чтобы провода, по которым возможно открывание замка, были недоступны снаружи.

- Контроллер должен иметь резервный источник питания на случай отключения электропитания.

- Предпочтительно использовать считыватель в вандалозащищенном корпусе.

В составе автономной системы контроля доступа используются также электронные замки, передающие информацию по беспроводным каналам связи: в двери устанавливается механический замок с электронным управлением и встроенным считывателем. Замок по радиоканалу связан с хабом, который уже по проводам обменивается информацией с рабочей станцией, на которой установлено программное обеспечение.

Для автономной системы возможно использовать «обратный метод», когда на контрольных точках устанавливаются идентификаторы, а сотрудники отмечаются считывателем-контроллером, впоследствии данные передаются при первой возможности — появление связи у считывателя. Этот метод удобно использовать, например, в местах где отсутствует связь, возможность прокладки электропитания или других коммуникаций. Также "обратный метод" может использоваться для контроля патрулирования больших периметров: после обхода территории или по окончании смены охранник сдаёт на проверку контроллер, в котором записаны все пройденные контрольные точки с указанием последовательности прохода и времени прохода каждой точки.

10. Дополнительные средства для реализации систем контроля и управления доступом:

- SM модуль, который позволяет посылать SMS с информацией о проходе (используется, например, в школах).
- для сетевой СКУД (также некоторые автономные системы) – возможность удаленного управления по сети Интернет (например, для управления системой контроля доступа из центрального офиса, если предприятие имеет множество филиалов).
- комплекс для персонализации пластиковых карт (принтер для печати на пластиковой карте данных владельца, в том числе, фотографии).
- режим «антипассбэк» – если человек уже прошел на охраняемую территорию, то повторное предъявление его идентификатора на вход будет запрещено (пока карта не будет предъявлена на выход), что исключит возможность прохода по одной карте двух и более человек. При этом сетевая СКУД позволяет организовать такой режим на всех точках прохода, объединённых в сеть, что обеспечивает полнофункциональную защиту по всему периметру контролируемой территории.

Сферы применения систем контроля и управления доступом разнообразны:

- офисы компаний, бизнес-центры;
- банки;
- образовательные учреждения;
- промышленные предприятия;
- охраняемые территории;
- автостоянки и парковки;
- места проезда автотранспорта;
- частные дома, жилые комплексы, коттеджи;
- гостиницы и отели;
- общественные учреждения.

Указания к работе:

1. Определить места установки считывателя карт доступа.
2. Произведите запись кода в карту доступа таким образом, чтобы реализовать модель системы управления доступом:
   - карта преподавателя – имеет доступ (индикатор должен гореть зеленым).
   - карта студента – не имеет доступа (индикатор должен гореть красным).
3. Сформулируйте вывод по проделанной работе и подготовьте отчет по проделанной работе. Отчет должен содержать:
   - цель работы;
   - задачи работы;
   - описание работы;
   - ход работ, включая пошаговую фиксацию проделанных действий;
   - вывод.

Вопросы для самоконтроля:

1. Что такое система контроля и управления доступа? Дайте определение понятию.

2. Объясните принцип функционирования системы контроля и управления доступом, созданной на основе считывателей и карт доступа.

3. На каком расстоянии считыватель способен считать код карты доступа?

4. Какие внешние (искусственные) помехи могут помешать считыванию кода с карты доступа?

5. Какие существуют виды карт доступа? Назовите их основные сходства и различия.

ОФОРМЛЕННЫЙ ОТЧЕТ НЕОБХОДИМО ВЫЛОЖИТЬ В ИНФОРМАЦИОННЫЙ РЕСУРС ТАЙМЛАЙН В СООТВЕТСТВУЮЩИЙ РАЗДЕЛ ПО ДИСЦИПЛИНЕ

Лабораторная работа № 6
«Подбор компонентов для заданной комплексной системы безопасности»

Цель работы: получить теоретические и практические навыки по проектированию комплексных систем безопасности, с учетом требований предъявляемых этим системам.

Задачи работы:

1. Спроектировать комплексную систему безопасности в заданном помещении, которая включает в себя подсистемы: видеонаблюдения, охранная и пожарная сигнализация, система контроля и управления доступом.
2. Произвести оптимизацию систем, предложенных к проектированию.
3. Произвести подбор рекомендуемого к установке оборудования.
4. Выполнить описание технических характеристик, используемого оборудования.
5. Оценить стоимость спроектированной комплексной системы безопасности.
6. Оформить отчет по проделанной работе.

Используемое оборудование: персональный компьютер с предустановленной операционной системой Windows 8.

Теоретические сведения:

Существует большое количество угроз, которые вынуждают руководство организаций принимать меры по их устранению с целью чего создаются системы комплексной безопасности.

1. Системы видеонаблюдения. Современные системы видеонаблюдения, применяемые на промышленных предприятиях - это интеллектуальный, высокотехнологичный продукт, позволяющий не только вести видеонаблюдение и видеорегистрацию, но и оперативно реагировать на

возникающие угрозы. Интеллектуальные возможности устанавливаемых Гран При систем позволяют:

- контролировать перемещения людей и транспортных средств в охраняемой зоне;
- своевременно обнаруживать оставленные без присмотра предметы;
- отслеживать факты пересечения границ охраняемых зон в выбранном направлении;
- фиксировать начало и прекращение движения в заданной зоне.

2. Система контроля и управления доступом. Проектируемые и устанавливаемые компанией Гран При системы контроля и управления доступом позволяют решать следующие задачи на территории промышленных предприятий:

- контролировать использование рабочего времени сотрудниками: приход/уход, обеденный перерыв, перекуры, служебные командировки.
- вести учет рабочего времени;
- ограничивать доступ в особо охраняемые зоны;
- контролировать въезд и выезд автотранспорта с территории предприятия.

3. Система охранно-пожарной сигнализации. Основные возможности систем охранно-пожарной сигнализации:

- своевременное оповещение дежурного о попытке несанкционированного проникновения;
- обнаружение очагов возгорания и задымления, включение системы пожаротушения, оповещения и эвакуации;
- передача информации о возгорании на пульт пожарной службы;
- выявлять случаи нарушения периметра;
- получать подтверждение фактов нарушения;

- оперативно передавать информацию на пульт дежурного с указанием места и времени предполагаемого нарушения.

Указания к работе:

1. На основании заданной преподавателем аудитории, выполните действия по замеру длины, ширины и высоты аудитории.

2. Согласно полученным данным, определите необходимые технические подсистемы, которые необходимы для реализации комплексной системы безопасности для заданной аудитории. Укажите их необходимость и значимость в составе комплексной системе защиты аудитории. Планируемыми к установке подсистемами являются:

- подсистема видеонаблюдения;
- подсистема охранной сигнализации;
- подсистема пожарной сигнализации;
- подсистема контроля и управления доступа.

3. Определите функции, которые будет выполнять каждая из подсистем, а также их опишите алгоритм из функционирования в случаях наступления чрезвычайной ситуации, в случае наблюдения.

4. Выполните подбор рекомендуемого оборудования, необходимого для реализации заданной системы комплексной безопасности в указанной аудитории и приведите их технические характеристики.

5. Разработайте схему (план) установки подобранного оборудования для реализации комплексной безопасности в аудитории (для каждой из подсистем по отдельности).

6. Произведите подсчет стоимости закупаемого оборудования (подготовьте смету закупки на оборудование).

7. Сформулируйте вывод по проделанной работе и подготовьте отчет по проделанной работе. Отчет должен содержать:

- цель работы;
- задачи работы;
- описание работы;

- ход работ, включая пошаговую фиксацию проделанных действий;
- вывод.

Вопросы для самоконтроля:

1. Дайте определение понятию «система видеонаблюдения». Назовите осуществляемые системой функции.
2. Дайте определение понятию «система контроля и управления доступом». Назовите осуществляемые системой функции.
3. Дайте определение понятию «система охранно-пожарной сигнализации». Назовите осуществляемые системой функции.
4. Чем характеризуется осуществление комплексной безопасности?
5. Что такое комплексная система безопасности? Охарактеризуйте понятие.

ОФОРМЛЕННЫЙ ОТЧЕТ НЕОБХОДИМО ВЫЛОЖИТЬ В ИНФОРМАЦИОННЫЙ РЕСУРС ТАЙМЛАЙН В СООТВЕТСТВУЮЩИЙ РАЗДЕЛ ПО ДИСЦИПЛИНЕ

Самостоятельная работа студентов

Задание. Подготовить реферат-доклад и презентацию по теме, согласно заданному варианту (см. таблица 1), который определяется порядковым номером студента по списку.

Цель работы: сбор и систематизация знаний по заданной теме.

Задачи работы:

1. Изучить и подобрать материал по теме.
2. Подготовить реферат-доклад.
3. Подготовить сопроводительную презентацию.
4. Выполнить защиту реферата.
5. Поделиться полученным результатами с аудиторией.

Таблица 1

Вариант задания

№	Тема доклада
1	Комплексные системы безопасности
2	Законодательная база систем безопасности
3	Охранные системы безопасности
4	Системы контроля и управления доступом
5	Системы видеонаблюдения
6	Пожарная система безопасности
7	Системы сбора и обработки в комплексных системах безопасности
8	Системы оповещения и громкой связи
9	Требования при проектировании систем безопасности
10	Контрольно-пропускные системы
11	Системы управления зданием
12	Архитектуры комплексных систем безопасности
13	Интерфейсы, применяемые при создании комплексных систем безопасности
14	Факторы, влияющие на организацию комплексной системы безопасности
15	Беспилотные летательные аппараты как средства комплексной систем защиты
16	Направления развития комплексных систем безопасности

Указания к работе: реферат и презентация должны быть оформлены согласно требованиям, представленным в приложении. Требования к презентации содержатся в приложении 1. Требования к реферату содержатся в приложении 2.

ОФОРМЛЕННЫЙ РЕФЕРАТ И ПРЕЗЕНТАЦИЮ НЕОБХОДИМО ВЫЛОЖИТЬ В ИНФОРМАЦИОННЫЙ РЕСУРС ТАЙМЛАЙН В СООТВЕТСТВУЮЩИЙ РАЗДЕЛ ПО ДИСЦИПЛИНЕ

Приложение

Приложение 1

Требования к презентации

Требования к содержанию мультимедийной презентации:

- соответствие содержания презентации поставленным дидактическим целям и задачам;
- соблюдение принятых правил орфографии, пунктуации, сокращений и правил оформления текста (отсутствие точки в заголовках и т.д.);
- отсутствие фактических ошибок, достоверность представленной информации;
- лаконичность текста на слайде;
- завершенность (содержание каждой части текстовой информации логически завершено);
- объединение семантически связанных информационных элементов в целостно воспринимающиеся группы;
- сжатость и краткость изложения, максимальная информативность текста;
- расположение информации на слайде (предпочтительно горизонтальное расположение информации, сверху вниз по главной диагонали; наиболее важная информация должна располагаться в центре экрана; если на слайде картинка, надпись должна располагаться под ней; желательно форматировать текст по ширине; не допускать «рваных» краев текста);
- наличие не более одного логического ударения: краснота, яркость, обводка, мигание, движение;
- информация подана привлекательно, оригинально, обращает внимание комиссии.

Требования к визуальному и звуковому ряду:

- использование только оптимизированных изображений (например, уменьшение с помощью MicrosoftOfficePictureManager, сжатие с помощью панели настройки изображения MicrosoftOffice);
- соответствие изображений содержанию;
- соответствие изображений возрастным особенностям слушателей;
- качество изображения (контраст изображения по отношению к фону; отсутствие «лишних» деталей на фотографии или картинке, яркость и контрастность изображения, одинаковый формат файлов);
- качество музыкального ряда (ненавязчивость музыки, отсутствие посторонних шумов);
- обоснованность и рациональность использования графических объектов.

Требования к тексту:

- читаемость текста на фоне слайда презентации (текст отчетливо виден на фоне слайда, использование контрастных цветов для фона и текста);
- кегль шрифта соответствует возрастным особенностям слушателей и должен быть не менее 24 пунктов;
- отношение толщины основных штрихов шрифта к их высоте ориентировочно составляет 1:5; наиболее удобочитаемое отношение размера шрифта к промежуткам меж¬ду буквами: от 1:0,375 до 1:0,75;
- использование шрифтов без засечек (их легче читать) и не более 3-х вариантов шрифта;
- длина строки не более 36 знаков;
- расстояние между строками внутри абзаца 1,5, а между абзацев – 2 интервала;
- подчеркивание используется лишь в гиперссылках.

Требования к дизайну:

- использование единого стиля оформления;

- соответствие стиля оформления презентации (графического, звукового, анимационного) содержанию презентации;
- использование для фона слайда психологически комфортного тона;
- фон должен являться элементом заднего (второго) плана: выделять, оттенять, подчеркивать информацию, находящуюся на слайде, но не заслонять ее;
- использование не более трех цветов на одном слайде (один для фона, второй для заголовков, третий для текста);
- соответствие шаблона представляемой теме (в некоторых случаях может быть нейтральным);
- в правом нижнем углу нумерация слайдов;
- целесообразность использования анимационных эффектов.

Требования к качеству навигации:

- работоспособность элементов навигации;
- качество интерфейса;
- целесообразность и рациональность использования навигации;
- цикличность презентации.

Требования к эффективности использования презентации:

- творческий, оригинальный подход к созданию презентации.

Сопроводительная речь:

- в заметках к каждому слайду в первой строке указывается время, затрачиваемое на речь, например – 10 сек. Выделить жирным;
- со второй строки пишется речь для слайда, соблюдая все правила русского языка.

Последовательность слайдов:

- слайд – «Титульный лист», должен содержать информацию аналогичную титульному листу пояснительной записки ВКР;
- слайд(ы) – Цель (и) и задачи.». Если все не входит на один слайд разбить на несколько;

- слайды основной части. Презентуют вашу проделанную работу;
- слайд(ы) – «Основные результаты.» Перечисляются основные результаты, выполненные в работе. Если есть акт внедрения вывести в конце на слайд с использованием анимации;
- слайд – «Все задачи решены. Цель достигнута.»;
- слайд – «Спасибо за внимание».
- Презентация не должна быть скучной, монотонной, громоздкой (оптимально это 10 – 15 слайдов на 7 мин максимум).

Приложение 2

Требования к реферату

Требования к структуре реферата по ГОСТ 7.32-2001 «Отчет о научно-исследовательской работе. Структура и правила оформления». Пункт 5.3. Реферат.

Приложение 3

Пример титульного листа

Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Российский государственный профессионально-педагогический
университет»
Институт инженерно-педагогического образования
Кафедра информационных систем и технологий

Отчет
по лабораторной работе №___
«название лабораторной работы»

Выполнил: студент группы XX–XXX
Фамилия Имя Отчество

Проверил: должность, ученое звание преподавателя
Фамилия Имя Отчество
Дата проверки: «___» _____ 2017 г.

Екатеринбург
2017