Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования «Кабардино-Балкарский государственный университет им. Х.М. Бербекова»
(КБГУ)

Институт электроники, робототехники и искусственного интеллекта

УТВЕРЖДАЮ

Руководитель ОПОП

_____ **Р.Ш. Тешев**

«12» февраля 2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ
Б1.В.13. МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ОБЪЕКТОВ

Направление подготовки
по специальности

11.05.01 Радиоэлектронные системы и комплексы

Специализация
Радиоэлектронные системы передачи информации

Квалификация выпускника
Инженер

Нальчик 2025

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Таблица 1

Код и формулировка компетенции	Индикаторы достижения	Планируемые результаты обучения по дисциплине (ЗУН)
ПК-4. Способен к проведению диагностики, оценки качества и надежности в процессе эксплуатации радиоэлектронных систем и комплексов.	**ПК-4.1.** Способен учитывать специфику и особенности различного назначения радиоэлектронных систем и комплексов при оценке эффективности работы функциональных узлов и частей радиоэлектронной аппаратуры. **ПК-4.2** Способен контролировать проведение диагностики и определять категории оценки качества на надежность, долговечность и безотказность работы радиоэлектронных систем и их составных частей.	**Знать** специфику и особенности различного назначения радиоэлектронных систем и комплексов при оценке эффективности работы функциональных узлов и частей радиоэлектронной аппаратуры. **Уметь** контролировать проведение диагностики радиоэлектронных систем и их составных частей. В**ладеть** методами оценки качества на надежность, долговечность и безотказность работы радиоэлектронных систем и их составных частей.
ПК-5. Способен осуществлять эксплуатацию и техническое обслуживание радиоэлектронных систем и комплексов.	**ПК-5.1** Способен осуществлять эксплуатацию радиоэлектронных систем и комплексов. **ПК-5.2** Способен осуществлять техническое обслуживание радиоэлектронных систем и комплексов.	**Знать** аппаратуру обслуживаемых радиоэлектронных систем и комплексов и её функционирование **Уметь** осуществлять эксплуатацию и техническое обслуживание радиоэлектронных систем и комплексов. **Владеть** навыками эксплуатации и технического обслуживания.

2 Шкала оценивания планируемых результатов обучения

2.1 Текущий контроль

Оценка результатов текущей успеваемости в рамках контрольных точек осуществляется посредством 70-балльной системы, при этом за добросовестное посещение занятий обучающийся может набрать до 10 баллов, за качественное прохождение оценочных мероприятий - до 60 баллов.

Таблица 2

Карта распределения рейтинговых баллов в рамках текущего контроля в 9 семестре

№	Оценочное средство	Форма проведения	Порядок проведения	Максимальное количество баллов	Критерии оценивания

1	Лабораторная работа №1 «Автономная система контроля доступа для одной двери на базе контроллера AX100».	смешанная	Работа включает в себя комплекс заданий, выполняется студентами попарно.	4	4- все задания выполнены верно, выводы по работе обоснованы; 3-2 - все задания выполнены верно, выводы по работе некорректны; 1 – задания выполнены частично или одно из заданий выполнено не верно, выводы содержат ошибки. 0 – задания не выполнены или все задания выполнены неверно
2	Лабораторная работа №2 «Интеллектуальная охранная система RiDom».	смешанная	Работа включает в себя комплекс заданий, выполняется студентами попарно.	4	4- все задания выполнены верно, выводы по работе обоснованы; 3-2 - все задания выполнены верно, выводы по работе некорректны; 1 – задания выполнены частично или одно из заданий выполнено не верно, выводы содержат ошибки. 0 – задания не выполнены или все задания выполнены неверно
3	Лабораторная работа №3 «Автоматическая система пожаротушения на базе блока управления АСПТ»	смешанная	Работа включает в себя комплекс заданий, выполняется студентами попарно.	4	4- все задания выполнены верно, выводы по работе обоснованы; 3-2 - все задания выполнены верно, выводы по работе некорректны; 1 – задания выполнены частично или одно из заданий выполнено не верно, выводы содержат ошибки. 0 – задания не выполнены или все задания выполнены

					неверно
4	Лабораторная работа №4 «Считыватели для системы контроля доступа».	смешанная	Работа включает в себя комплекс заданий, выполняется студентами попарно.	4	4- все задания выполнены верно, выводы по работе обоснованы; 3-2 - все задания выполнены верно, выводы по работе некорректны; 1 – задания выполнены частично или одно из заданий выполнено не верно, выводы содержат ошибки. 0 – задания не выполнены или все задания выполнены неверно
5	Лабораторная работа №5 ««Интеллектуальная охранная GSM система SAPSAN® GSM PRO 2».».	смешанная	Работа включает в себя комплекс заданий, выполняется студентами попарно.	4	4- все задания выполнены верно, выводы по работе обоснованы; 3-2 - все задания выполнены верно, выводы по работе некорректны; 1 – задания выполнены частично или одно из заданий выполнено не верно, выводы содержат ошибки. 0 – задания не выполнены или все задания выполнены неверно
1	Лабораторная работа №6 «Система контроля и управления доступом ВЕРСЕТ – GSM 03ВМ».	смешанная	Работа включает в себя четыре задания, выполняется студентами попарно.	4	3- все задания выполнены верно, выводы по работе обоснованы; 2 - все задания выполнены верно, выводы по работе некорректны; 1 – задания выполнены частично или одно из заданий выполнено не верно, выводы содержат ошибки. 0 – задания не

					выполнены или все задания выполнены неверно
2	Практическая работа №1 «Системы IP и аналогового видеонаблюдения».	смешанная	Работа включает в себя четыре задания, выполняется студентами попарно.	3	3- все задания выполнены верно, выводы по работе обоснованы; 2 - все задания выполнены верно, выводы по работе некорректны; 1 – задания выполнены частично или одно из заданий выполнено не верно, выводы содержат ошибки. 0 – задания не выполнены или все задания выполнены неверно
3	Практическая работа №2 «Цветной видеодомофон Falcon eye fe-70ch orion».	смешанная	Работа включает в себя четыре задания, выполняется студентами попарно.	3	3- все задания выполнены верно, выводы по работе обоснованы; 2 - все задания выполнены верно, выводы по работе некорректны; 1 – задания выполнены частично или одно из заданий выполнено не верно, выводы содержат ошибки. 0 – задания не выполнены или все задания выполнены неверно
4	Практическая работа №3 «Биометрические системы аутентификации. Контроллер BioSmart 4-O».	смешанная	Работа включает в себя четыре задания, выполняется студентами попарно.	3	3- все задания выполнены верно, выводы по работе обоснованы; 2 - все задания выполнены верно, выводы по работе некорректны; 1 – задания выполнены частично или одно из заданий выполнено не верно, выводы содержат

					ошибки. 0 – задания не выполнены или все задания выполнены неверно
5	Практическая работа №4 «Интеллектуальная охранная система RiDom».	смешанная	Работа включает в себя четыре задания, выполняется студентами попарно.	3	4- все задания выполнены верно, выводы по работе обоснованы; 3-2 - все задания выполнены верно, выводы по работе некорректны; 1 – задания выполнены частично или одно из заданий выполнено не верно, выводы содержат ошибки. 0 – задания не выполнены или все задания выполнены неверно
	Практическая работа №5 «Считыватели для системы контроля доступа»	смешанная	Работа включает в себя четыре задания, выполняется студентами попарно.	4	4- все задания выполнены верно, выводы по работе обоснованы; 3-2 - все задания выполнены верно, выводы по работе некорректны; 1 – задания выполнены частично или одно из заданий выполнено не верно, выводы содержат ошибки. 0 – задания не выполнены или все задания выполнены неверно
	Тесты по 1 контрольной точке	с применением ДТ	Студент проходит компьютерное тестирование в ЭИОС.	5	Количество баллов пропорционально количеству правильных ответов
12	Тесты по 2 контрольной точке	с применением ДТ	Студент проходит компьютерное тестирование в ЭИОС.	5	Количество баллов пропорционально количеству правильных ответов
14	Коллоквиум по 1 контрольной точке	письменная	Студенты отвечают	5	10-8– ответы полные, точные,

			письменно на вопросы коллоквиума		демонстрируют глубокое понимание темы, аргументация логична; 7-5 – ответы в основном правильные, но содержат незначительные ошибки; 4-3- ответы недостаточно полные; 2 – ответы частичные, содержат ошибки или требуют наводящих вопросов; 1-ответы не на все вопросы, частичные. 0 – ответы отсутствуют или полностью неверные.
	Коллоквиум по 2 контрольной точке	письменная	Студенты отвечают письменно на вопросы коллоквиума	5	10-8– ответы полные, точные, демонстрируют глубокое понимание темы, аргументация логична; 7-5 – ответы в основном правильные, но содержат незначительные ошибки; 4-3- ответы недостаточно полные; 2 – ответы частичные, содержат ошибки или требуют наводящих вопросов; 1-ответы не на все вопросы, частичные. 0 – ответы отсутствуют или полностью неверные.
	Итого:			**60**	

Карта распределения рейтинговых баллов в рамках промежуточной аттестации

№	Оценочное средство	Форма проведения	Порядок проведения	Максимальное количество баллов	Критерии оценивания
1	Билет для опроса	Устный опрос	Билет содержит 3 теоретических вопроса. На	Теоретические вопросы – 30 баллов. .	**Критерии оценивания теоретических вопросов:**

			теоретические вопросы студент должен ответить устно.		25 до 30 баллов: Глубокий уровень владения материалом, точное знание ключевых концепций, способность анализировать и интерпретировать факты, грамотно строить высказывания, привести примеры, свободно оперировать терминологией. От 19 до 24 баллов: Базовое владение предметом, умение последовательно раскрыть основную мысль вопроса, грамотное применение терминов, наличие существенных элементов анализа и обобщений, но недостаточное развертывание или отдельные неточности. От 13 до 18 баллов: Частичное освоение материала, попытка объяснить основной смысл вопроса, использование некоторых базовых терминов, но отсутствие глубокого понимания сложных моментов, логические недостатки изложения, отсутствие выводов. От 7 до 12 баллов: Ошибочные представления, слабо

					выраженное владение основными понятиями, значительные затруднения в интерпретации вопросов, существенные фактологические ошибки, отсутствие обоснованных выводов и примеров. От 0 до 6 баллов: Полное непонимание темы, неспособность сформулировать адекватный ответ, грубые ошибки, несоответствие требованиям задания.

3. Оценочные материалы для текущего и промежуточного контроля успеваемости
3.1. Оценочные материалы для текущего контроля

Лабораторная работа №1
Автономная система контроля
доступа для одной двери на базе контроллера AX100

Цель работы: изучить работу автономной системы контроля доступа для одной двери на базе контроллера AX100

Порядок выполнения

В комплект учебного стенда AX100 входят:

1) контроллер AX100;
2) считыватель бесконтактных карт;
3) десять бесконтактных карт или брелоков;
4) мастер-карта для программирования системы;
5) комплект креплений;
6) программное обеспечение для программирования, управления и мониторинга системы;
7) кабель для подключения к компьютеру.

Действия по конфигурированию системы СКУД выполняются в программе, для чего необходимо загрузить в ПК программу AX100. Выбрать язык – English и вид интерфейса Windows Classic или Graphitic Style. Классический стиль Windows™ наиболее подходит для старых ПК и ноутбуков с объемом оперативной памяти всего 64 МБ и разрешением видео 800 x 600. Графический пользовательский интерфейс делает его легким в использовании и работе.

Используя User Name и Password войдите в систему. После загрузки изучите интерфейс. Имя пользователя по умолчанию для AX100 – "1" и пароль – "1". Имена пользователей и пароли не чувствительны к регистру.

Выполните тестирование системы с помощью тестового мастера. Тестовый мастер можно выбрать из выпадающего списка «Инструменты» в верхней части меню.

Тестовый мастер проведет полное тестирование оборудования, карт и программного обеспечения. Надо ввести номер карты в поле ниже (Please type the card number in the box below).

На экране Тестового мастера выберите тип карты из списка карт, которые хотите протестировать, и нажмите «Далее». Убедитесь, что контроллер AX100 еще подключен к ПК – теперь мастер тестирования выполнит проверку и свяжется с контроллером. Если контроллер работает правильно, на экране отобразится зеленая галочка. Тестовый мастер теперь запросит, чтобы карта была вставлена или представлена считывателю.

Появится сообщение: Пожалуйста, предъявите свою тестовую карту считывателю (Please present yout test card to the reader). Далее – ожидание данных карты (Waiting for card data) и, наконец, появится информация о карте (The card information).

Тестовый мастер проверит формат карты, код устройства и номер карты. Нажмите «Далее (Next)», чтобы продолжить. Тестовый мастер теперь настроит формат карты, держателя карты, точку доступа и загрузит данные в контроллер. Для продолжения нажмите «Далее», после чего Тестовый мастер проведет полный набор аппаратных тестов.

* *Разблокировка двери*. Поднесите вашу карту к считывателю один раз – это разблокирует дверь. Светодиод контроллера должен гореть зеленым в течение 5 с.

* *Режим высокой безопасности.* Поднесите вашу карту к считывателю 4 раза – это протестирует режим высокой безопасности. Светодиод контроллера будет мигать красным 4 раза каждые 5 с.

* *Нормальный режим.* Поднесите вашу карту к считывателю снова 4 раза – это вернет систему в нормальный режим. Светодиод контроллера будет мигать зеленым каждые 5 с.

* *Открытие защелки двери.* Поднесите вашу карту к считывателю дважды – это откроет защелку двери. Светодиод контроллера будет мигать зеленым дважды каждые 5 с.

* *Блокировка двери.* Поднесите вашу карту к считывателю дважды снова – это заблокирует дверь. Светодиод контроллера будет мигать зеленым каждые 5 с. Нажмите «Далее», чтобы продолжить (см. Приложение).

Создайте карту доступа и выполните ее основные настройки.

Поля базы данных для держателя карты. Номер карты и группа доступа являются минимальными полями, необходимыми для активации карты. Все остальные поля базы данных являются необязательными и сгруппированы в несколько удобных для навигации вкладок.

Функция «Карта 0». Данные о держателе карты остаются в системе без удаления информации. Эта функция особенно полезна для частых посетителей. Измените номер карты на 0, когда человек уходит. По возвращении измените номер карты с 0 на фактический номер выданной карты.

Выполните настройку контроллера (см. Приложение).

Доступ и конфигурация. Каждый контроллер имеет свой серийный номер, который используется для связи с ПК. Если идентификатор был введен вручную во время настройки системы или, когда контроллеры подключены с помощью DTU, функция замены должна использоваться, когда контроллеры находятся в рабочем состоянии.

Имя точки доступа. Это логическое имя, которое пользователь присваивает каждому контроллеру, например, «входная дверь» или «подача товаров».

Расширенная длина поля позволяет ввести до 50 символов, например, «Здание 1 Секция Западная дверь 28 Администрация». Первые 20 символов отображаются в текущей информации о контроллере.

Комментарии к двери. Это поле может хранить дополнительные подробности касательно расположения или любой другой информации, например, временно не используется в связи со строительными работами.

Время открытия двери. Три настройки:
* *Время открытия двери (1–255 с)*: количество времени, на которое дверь будет открыта при использовании действительной карты.
* *Расширенное время (1–255 с)*: позволяет отдельным держателям карт открывать дверь на более длительный период времени, например, для пожилых людей или людей с ограниченными возможностями.
* *Запрос на выход (1–255 с)*: это время может быть индивидуально настроено и часто устанавливается на более длительное время, когда REX используется на стойке регистрации, позволяя посетителям немного увеличить время входа.

При использовании кнопки REX считыватель устанавливается снаружи и может издавать звуковой сигнал дважды, чтобы указать, что дверь была открыта для посетителей. Эта функция особенно полезна при использовании с магнитными замками, так как их работа полностью бесшумна.

Настройки режима запуска. Эти настройки позволяют определить, как будет работать дверь в случае полного отключения электроэнергии, включая разряд батареи резервного питания. Все данные хранятся постоянно в контроллере. Могут храниться без питания. При включении питания они продолжат работу без необходимости загрузки базы данных.
* *Режим высокой безопасности*: доступ будут иметь только держатели карт с высоким уровнем безопасности.
* *Нормальный режим*: возврат к нормальному режиму от состояния, в котором дверь находилась до отключения электроэнергии.
* *Дверь разблокирована*: дверь остается разблокированной, пока не будет предъявлена действительная карта с функцией разблокировки дважды или дверь не будет изменена на нормальный режим через ПК.
* *Последний известный режим*: возвращает статус двери к тому состоянию, которое было до отключения электроэнергии.

Настройки дверного контакта. К контроллеру можно подключить стандартный дверной контакт (нормально разомкнутый), используемый в системах охранной сигнализации. Статус двери может быть виден в реальном времени на экране (только онлайн) и предоставляет дополнительные функции для выбора.
* *Дверной контакт*: включен или выключен.
* *Дверь взломана*: если дверь открыта без REX или действительной карты, это вызовет тревогу. При подключении к ПК, это отобразится на экране транзакций, позволяя удаленно перезагрузить систему. Считыватель будет активирован на 2 минуты и автоматически остановится. Сброс также может быть выполнен с помощью действительной карты. Когда дверь закрывается, функция автоматически включается снова.
* *Отключить звуковой сигнал*: эта функция отключает звуковую сигнализацию считывателя при закрытии офиса.
* *Считыватель выключен при открытии*: считыватель будет отключен (не REX), если контакт двери открыт. Эту функцию можно использовать для систем сигнализации.
* *Сигнализация открытой двери*: время после истечения реле, когда дверь может быть открыта до подачи сигнала тревоги.
* *Местная активация сигнализации*: активирует сигнализацию считывателя без отправки сигнала тревоги на ПК (если он онлайн). Эта функция обычно используется вместе с сигнализацией открытой двери и предупреждает людей о необходимости закрыть дверь.
* *Сброс реле*: деактивирует реле таймера мгновенно при открытии двери.
Это увеличивает безопасность, избегая разблокированной двери на определенное количество секунд после того, как человек уже прошел через нее.

Настройки PIN-кода. Контроллеры работают в различных режимах и могут быть изменены без необходимости перезагрузки системы.

Режимы работы

* *Только карта*: действительная карта необходима для открытия двери в этом режиме. Система поддерживает 4000 индивидуальных владельцев карт на контроллере AX100.
* *Только PIN-код*: для открытия двери требуется только персональный идентификационный номер (PIN-код). Это может быть индивидуальный номер для пользователя или номер для группы пользователей. Система поддерживает только 2000 PIN-кодов или пользователей карт и PIN-кодов.
* *Карта + PIN-код*: действительная карта должна быть представлена считывателю после ввода индивидуального PIN-кода держателя карты. В этом режиме контроллер определяет длину PIN-кода на карте и не требует ввода символа #.
* *Время ожидания PIN-кода*: указывает время в секундах для ввода PIN-кода перед очисткой буфера или отправкой данных как неверных или неполных.
* *Высокий уровень безопасности активирует PIN-код*: система работает в режиме «Только карта» и переходит в режим «Карта + PIN-код», когда карта высокого уровня безопасности используется четыре раза на считывателе.

Произведите резервное копирование.

Программное обеспечение имеет встроенную утилиту резервного копирования. Резервные копии могут создаваться автоматически в установленные сроки или вручную с поддержкой сетевого резервного копирования. Резервные копии старых версий ПО автоматически преобразуются, что позволяет избежать необходимости выполнять шаги для восстановления программного обеспечения. Автоматические резервные копии нумеруются с использованием даты и времени их создания. Для удаления старых резервных копии надо выделить соответствующий файл, нажать клавишу «Удалить» и подтвердить это действие. Надо создать полное резервное копирование системы сразу после того, как все системные настройки были внесены.

Для создания резервной копии перейдите к восстановлению, выделите новый созданный файл, щелкните правой кнопкой мыши и выберите «Переименовать» – переименуйте файл, например, в «Мастер настройки».

Эта резервная копия позволит восстановить систему до ее первоначальных настроек. Для автоматического резервного копирования не нужно закрывать экран программы или держатель карты. Частичные резервные копии также могут быть выбраны только для файлов базы данных.

После выполнения перечисленных операций произведите проверку работоспособности СКУД для чего выполните вход по сформированной карте доступа, а выход по нажатию кнопки «Выход».

Контрольные вопросы

1. Назначение и характеристика бесконтактных карт доступа и бесконтактных Smart-карт.
2. Отличие бесконтактных Smart-карт и proximity-карт.
3. Пластиковые магнитные карты.
4. Штрихкодовая технология. Wiegand-технология.
5. Функции и возможности автономной системы контроля доступа на базе контроллера AX100.
6. Возможности функции «подключи и работай» (Plug & Play).
7. Какие входы предоставляет контроллер AX100.

Лабораторная работа №2
Интеллектуальная охранная система RiDom

Цель работы: получить теоретические знания и практические навыки по работе с интеллектуальной охранной системой «Защита дома RiDom».

Порядок выполнения работы

Скачайте мобильное приложение RiDom и установите, следуя указаниям в приложении. Запустите приложение RiDom. Следуйте указаниям в приложении, чтобы зарегистрировать подключенный HUB и создать объект. Заполните данные о вашем местоположении, серийный номер HUB (он расположен на корпусе HUB с обратной стороны), придумайте название для вашего объекта, например: «Дом».

После успешного подключения HUB, он отобразится в приложении RiDom на главном экране. Далее необходимо выбрать доступную Wi-Fi сеть 2.4 ГГЦ, на которую будет переключен центр управления для постоянной работы. Для этого зайти в раздел «Мои устройства» – «Ri-HUB-1», перейти в настройки «Беспроводное подключение (Wi-Fi)» и выбрать нужную сеть, указав соответствующий пароль безопасности.

Новые настройки подключения будут применены сразу без перезагрузки HUB. Выключите мобильную точку доступа на вашем смартфоне. Обратите внимание на светодиод Wi-Fi на плате HUB. Он снова должен включиться, что свидетельствует о работе HUB через роутер.

Внимание! Если ошиблись в пароле подключения и HUB не соединяется с вашим роутером, то установите перемычку на контакты RST до принудительной перезагрузки HUB. Настройки подключения сети будут сброшены на заводские. После этого вы сможете снова запустить мобильную точку доступа на своём смартфоне и повторить настройку сети. После завершения настройки подключения HUB к вашей домашней сети закройте корпус HUB.

Заполните данные о вашем местоположении.

Введите серийный номер HUB.

Дайте название вашему объекту.

Добавьте все устройства в систему.

Поставьте сконфигурированную систему на охрану и проверьте ее реакцию на срабатывание датчиков.

Добавьте другого пользователя по приглашению.

Передайте другому пользователю права на управление.

Контрольные вопросы

1. Что такое интеллектуальная системы защиты?
2. Объясните назначения прибора Ri-HUB в интеллектуальная системе.
3. Принцип работы датчиков движения и температуры Ri-MTD.
4. Принцип работы датчика открытия Ri-DO и датчик дыма Ri-SD.

ЛАБОРАТОРНАЯ РАБОТА № 3
Автоматическая система пожаротушения на базе блока управления АСПТ

Цель работы: получить теоретические знания и практические навыки по работе с системой автоматического пожаротушения.

Порядок выполнения работы

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 оповещения – 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, но точность определения места пожара низкая. Для небольших помещений это не важно. Стоимость всех элементов аналоговой сигнализации меньше адресной в разы. 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 является пожарная централь. При повреждении шлейфа выявление места обрыва или короткого замыкания затруднено.

Для повышения надежности работы и простоты эксплуатации сейчас применяется метод опроса по кольцу. 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:

1. газовые (углекислый газ, азот и др.);
2. водяные (тонкодисперсной воды);
3. пенные и водопенные (вода с пенообразователем);
4. порошковые (специальные порошки);
5. аэрозольные.

Системы дымоудаления бывают динамические и статические. Статическая это система отключения вентиляции, предотвращающая проникновение дыма в другие помещения. Динамические системы более эффективны. В них дым удаляется при помощи вытяжной вентиляции. Вентиляторы работают для удаления дыма и для подачи свежего воздуха. 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.

1. Произвести тестирование работоспособности приборов и извещателей, входящих в состав системы пожаротушения.
2. Перевести системы в режим охраны.
3. Смоделировать ситуацию «Пожар».
4. Вывод по проделанной работе и подготовить отчет о проделанной работе.

5. Отчет должен содержать: цель работы, задачи работы, описание работы, ход работ, включая пошаговую фиксацию проделанных действий, выводы.

Контрольные вопросы

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. Классификация автоматических систем пожаротушения.
5. Объясните назначения прибора АСПТ в системе автоматической пожарной сигнализации.

ЛАБОРАТОРНАЯ РАБОТА № 4
Считыватели для системы контроля доступа

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

Порядок выполнения работы

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:

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).

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

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

Устанавливающиеся на проходах/проездах.

Турникеты – используются на проходных предприятиях, 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 планками «антипаника» – планками, переламывающимися усилием нормального человека (требование пожарной инспекции).

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

Ворота и шлагбаумы – устанавливаются на въездах на территорию предприятия, на автомобильных парковках и автостоянках, на въездах на придомовую территорию, во дворы жилых зданий.

Основное требование – это устойчивость к климатическим условиям и возможность автоматизированного управления при помощи системы контроля доступа. При организации контроля доступа проезда к системе предъявляются дополнительные требования – повышенная дальность считывания меток, распознавание автомобильных номеров в случае интеграции с системой видеонаблюдения.

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

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 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. 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.

1. Проверить работоспособность считывателей, контроллера, преобразователя интерфейсов, аккумулятора, ключа, геркона, карт, проводов.
2. Коммутировать компоненты СКУД согласно схеме.
3. Запитать систему от аккумулятора.
4. Подключить систему к компьютеру.
5. Подключить считыватель Proxy 5MS-USB к компьютеру.
6. Загрузить программу SecurityCoder.
7. Запрограммировать одну карту типа «Мастер» согласно инструкции.
8. Запрограммировать 2-3 карты типа «Пользователь» с режимом работы «Передача кода карты после успешной авторизации к сектору».
9. Произвести настройку систему контроля и управления доступом в заданном помещении.
10. Проверить работоспособность настроенной системы.

11. Произвести 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).

12. Оформить отчет по проделанной работе.

Контрольные вопросы

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.

Лабораторная работа №6
Система контроля и управления доступом ВЕРСЕТ – GSM 03ВМ

Порядок выполнения работы

1. Ознакомиться с техническими характеристиками и возможностями прибора.
2. Получить у преподавателя охранные пожарные извещатели.
3. Собрать охранный и пожарный шлейфы, после чего осуществить их подключение при выключенном питании прибора.
4. Подключить прибор к ЭВМ с помощью USB-кабеля и выполнить конфигурирование полученной охранно-пожарной системы.
5. Выполнить регистрацию электронных ключей в базе прибора.
6. Записать созданную конфигурацию в память прибора.

Контрольные вопросы

1. Назначение и возможности прибора «ВЕРСЕТ – GSM 03ВМ»,
2. Перечислите внешние устройства, подключаемые к прибору
3. Опишите конструкцию прибора
4. Какие способы доставки по группам событий для телефонов
5. Как организована охрана от проникновения

Практическая работа №1
Системы IP и аналогового видеонаблюдения

1. Ознакомиться с теоретической частью: виды систем видеонаблюдения, виды и типы видеокамер и их характеристики. Ознакомиться с правилами построения ЛВС для систем IP-видеонаблюдения.
2. Подготовить к работе лабораторный стенд для IP-видеонаблюдения, для чего установить оборудование и подключить их к системе.
3. Настроить стенд.
4. Установить программу поиска видеокамер в локальной сети и организовать поиск подключенных программ. Записать IP-адреса обнаруженных программ.

Полностью скоммутированную систему необходимо настроить. Первым этапом нужно прописать в сетевой карте ПК IP-адрес видеокамеры. Для этого нужно перейти по следующему пути: «Панель управления\Сеть и Интернет\Сетевые подключения». В появившемся окне выбирать сетевой адаптер, к которому подключена видеокамера. Далее, двойным щелчком левой кнопки мыши по иконке открывается свойство адаптера. В появившемся диалоговом окне необходимо открыть пункт «IP версии 4 (TCP/IPv4)», после чего появляется окно настройки адресов камеры (рис. 2.3).

Далее прописывается IP-адрес камеры, указанный на панели самой камеры. На этом первый этап настройки сети завершён. Следующим шагом будет установка программного обеспечения.

5. Установить программу для видеонаблюдения VMS и подключиться к обнаруженным камерам. Получить изображения.

Контрольные вопросы.

1. Перечислите характеристики видеокамеры FE-IPC-BL200PVA.
2. Что входит в комплект рабочего стенда.
3. Какое значение имеет расположение камеры
4. Общие характеристики прибора

Практическая работа №2
Цветной видеодомофон Falcon Eye FE-70CH ORION

1. Ознакомиться с теоретической частью, посвященной описанию цветного видеодомофона Falcon Eye FE-70CH ORION, и с правилами безопасности его использования.
2. Выполнить просмотр видео от панели и видеокамер.
3. Осуществить внутренний вызов монитора (интерком), прослушивание мониторов.
4. Выполнить захват (сохранение) изображений: автоматический и ручной захват изображения.
5. Определить оптимальное место установки монитора.
6. Отрегулировать звонок от посетителя.
7. В дежурном режиме организовать просмотр видео от панелей и камер.
8. Передать информацию на все мониторы с помощью функции общего вызова**.**
9. Изучить функцию интеркома**.**
10. Выполнить настройку громкости, яркости, контрастности, цвета и формата изображения (4:3, 16:9).
11. В системных настройках произвести включение или выключение функции «Не беспокоить»
12. В режиме ожидания включить режим прослушивания другого монитора.
13. Освоить функцию «Системные настройки монитора».

Контрольные вопросы

1. Назначение и функции цветного видеодомофона falcon eye fe-70ch orion
2. Сколько мониторов параллельно к подъездной системе домофонии можно подключить
3. Какие настройки возможны в этой системе
4. С каким вызывными панелями работает этот прибор
5. В какое место нужно установить монитор

Практическая работа №3
Биометрические системы аутентификации. Контроллер BioSmart 4-O

1. Ознакомиться с теоретической частью, посвященной системе аутентификации и работе контроллера BioSmart 4-O.
2. Ознакомиться с правилами безопасности его использования.
3. Подготовить к работе лабораторный стенд для системы аутентификации и контроллера BioSmart 4-O.
4. Изучить и выполнить подключение дополнительного оборудования: ПК, БУР, Wiegand интерфейса контроллера и электромеханического замка.
5. Определить конфигурацию контроллеров Biosmart в ПО Biosmart-Studio.
6. Освоить работу раздела «Системные параметры».

7. Освоить регистрацию отпечатков пальцев. Зарегистрировать отпечаток пальца. Проверить на пропуск отпечаток пальца.

Контрольные вопросы

1. Принцип работы, технические характеристики контроллер BioSmart 4-O
2. Подключение какого дополнительного оборудования возможно
3. Какие контроллеры используются в этой работе
4. Перечислите системные параметры

Практическая работа №4
Интеллектуальная охранная система RiDom

1. Скачайте мобильное приложение RiDom и установите, следуя указаниям в приложении.
2. Запустите приложение RiDom.
3. Заполните данные о вашем местоположении.
4. Введите серийный номер HUB.
5. Дайте название вашему объекту.
6. Добавьте все устройства в систему.
7. Поставьте сконфигурированную систему на охрану и проверьте ее реакцию на срабатывание датчиков.
8. Добавьте другого пользователя по приглашению.
9. Передайте другому пользователю права на управление.

Контрольные вопросы

1. Что такое интеллектуальная системы защиты?
2. Объясните назначения прибора Ri-HUB в интеллектуальная системе.
3. Принцип работы датчиков движения и температуры Ri-MTD.
4. Принцип работы датчика открытия Ri-DO и датчик дыма Ri-SD.
5. Для чего предназначен центр управления «Ri-HUB-1»
6. Функции HUB
7. Из чего состоит комплект RiDom-Дача
8. Какие датчики здесь используются
9. Принцип действия датчика «Ri-SD-1»

Практическая работа №5
Считыватели для системы контроля доступа

1. Проверить работоспособность считывателей, контроллера, преобразователя интерфейсов, аккумулятора, ключа, геркона, карт, проводов.
2. Коммутировать компоненты СКУД согласно схеме.
3. Запитать систему от аккумулятора.
4. Подключить систему к компьютеру.
5. Подключить считыватель Proxy 5MS-USB к компьютеру.
6. Загрузить программу SecurityCoder.
7. Запрограммировать одну карту типа «Мастер» согласно инструкции.
8. Запрограммировать 2-3 карты типа «Пользователь» с режимом работы «Передача кода карты после успешной авторизации к сектору».
9. Произвести настройку систему контроля и управления доступом в заданном помещении.
10. Проверить работоспособность настроенной системы.
11. Произвести 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).

12. Оформить отчет по проделанной работе.

Контрольные вопросы

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.

Контрольная работа №1

Каждый обучающийся получит индивидуальный билет, включающий 3 вопроса. Перечень вопросов приведен ниже.

1. Исходные положения для разработки концепции обеспечения безопасности объектов.
2. Категории объектов охраны.
3. Требования к технической укрепленности объектов.
4. «Модель» нарушителя.
5. Пути и способы его проникновения на охраняемый объект.
6. Инженерные средства защиты.
7. Технические средства охраны.
8. Электронные средства: средства обнаружения, средства коммуникации.
9. ССОИ - аппаратно-центральная система обеспечения взаимодействия человека с комплексом технических средств.
10. Классификация ССОИ.
11. Функции ССОИ в составе комплексов технических средств охраны.
12. Структура построения ССОИ.
13. Пластиковые карточки, карточки со штрих-кодом, карточки с магнитной полосой, смарт-карты.

Контрольная работа 2

Каждый обучающийся получит индивидуальный билет, включающий 3 вопроса. Перечень вопросов приведен ниже.

1. Аудиодомофонные устройства.
2. Видеодомофонные устройства.
3. Системы контроля доступа.
4. Физические средства защиты.
5. Извещатели.
6. Приемно-контрольные приборы.
7. Системы передачи сообщений.
8. Резервные источники питания. Пожарная сигнализация.
9. Определение интегрированной системы охраны.
10. Структура и функции интегрированной системы охраны.
11. Выбор характеристик ИСО для конкретного объекта.
12. Интегрированная система охраны. Назначение системы. Функции системы.
13. Рекомендации по интерфейсу RS-485. Удлинение линии интерфейса RS-485 с помощью модемов.

14. Особенности применения систем видеонаблюдения. Телевизионные камеры н устройства для их оснащения.

Вопросы для тестирования

Тема 1. Концепция обеспечения безопасности объектов.

I: ТЗ № 1
S: Категории объектов защиты по степени важности делятся на
+:особо важные, важные, общего назначения.
-:Глобального, регионального, местного значения
-:Большие, средние, маленькие

I: ТЗ № 2
S: Различают следующие категории объектов защиты
а)по степени важности
б)по размеру нанесенного ущерба объекту, окружающей среде, общественным структурам
в)нанесение вреда здоровью и жизни людей, экологии и т.д.
г)по коммерческому ущербу
-:Только ответы а, б
-:Только ответы в, г
+:Все ответы верны

I: ТЗ № 3
S: Особенности задач охраны различных типов объектов (два верных ответа)
+:На ОВ объектах необходимо нейтрализовать злоумышленника до того, как он выполнит намеченные действия.
+:На ПК объектах нарушителя нейтрализовать как до, так и после совершения акции.
-:Реализовать только видеонаблюдение на объектах
-: На ОВ объектах нет необходимости нейтрализовывать злоумышленника
-: На ПК объектах нарушителя нейтрализовать только после совершения акции.
-: Реализовать только видеонаблюдение на объектах

I: ТЗ № 4
S: На объектах важно определить исходное положение нарушителя, так как (2 верных ответа)
+:На ОВ объектах нарушитель не должен находиться на территории объекта (недопустимо присутствие посторонних лиц).
+:На ПК объектах потенциальный нарушитель не может быть выявлен как злоумышленник, пока не совершит противоправные действия.
-: На ОВ объектах нарушитель может находиться на территории объекта.

I: ТЗ № 5
S: Основные задачи, решаемые физическими средствами защиты (верны 4 ответа):
+:Охрана территории, оборудования, внутренних помещений и наблюдение за ними.
-: Уборка территории предприятия.
+:Осуществление контролируемого доступа в контролируемые зоны.
+:Противопожарная защита.
+:Блокирование действий злоумышленника.
-: Оповещение всего населения об опасности.

I: ТЗ № 6
S: Адекватные меры защиты предусматривают:
а) тотальный контроль несанкционированного проникновения на территорию объекта, в здания и помещения;
б) ограничение и контроль доступа людей в «закрытые» здания и помещения с возможностью документирования результатов контроля;
в) обнаружение злоумышленника на самых ранних этапах его продвижения к цели акции;
г) оценку ситуации;
-:Верны только варианты а,б
-:Верны только варианты б,в
-:Верны только варианты в,г
+:Верны все варианты

I: ТЗ № 7
S: Адекватные меры защиты предусматривают:
а) обнаружение злоумышленника на самых ранних этапах его продвижения к цели акции;
б) создание на пути продвижения нарушителя физических препятствий, обеспечивающих задержку, необходимую силам охраны для его перехвата;
в) принятие немедленных действий по развертыванию сил охраны и пресечению действий злоумышленников;
г) видеодокументирование действий персонала на особо ответственных участках объекта.
-:Верны только варианты а,б
-:Верны только варианты б,в
-:Верны только варианты в,г
+:Верны все варианты

I: ТЗ № 8
S: Система охранно-тревожной сигнализации предназначена для
а) просмотра состояния охраняемых помещений на планах в графической форме на автоматизированных рабочих местах и отображения на них сигналов тревоги или неисправности;
б) ведение протокола событий системы ОТС в памяти компьютера с возможностью просмотра на мониторе и его распечатки;
в) ведение электронного журнала, фиксирующего действия операторов в стандартных и нештатных ситуациях.
-:Верны только варианты а,б
-:Верны только варианты б,в
+:Верны все варианты

I: ТЗ № 9
S: Система охранно-тревожной сигнализации обеспечивает:
а) интеграцию с другими системами ИСБ на программно-аппаратном уровне;
б) ручное или аппаратное управление постановкой/снятием с охраны с помощью электронных карт-пропусков;
в) контроль состояния системы с центрального пульта, мониторов АРМ постов охраны, и других АРМов в соответствии с регламентом;
-:Верны только варианты а,б
-:Верны только варианты б, в
-:Верны только варианты а,в
+:Верны все варианты

I: ТЗ № 10
S: Охранные радиоволновые извещатели – это
+: извещатели, излучающие в диапазоне ультракоротких радиоволн.
-:извещатели, которые обнаруживают тепловое излучение человеческого тела и формируют сигнал тревоги в случае, когда источник теплового излучения движется.
-:извещатели, излучающие ультразвуковые колебания и принимающие сигнал, отраженный от окружающих предметов. Формирование тревожного сигнала происходит в случае возникновения движения в контролируемой зоне.

I: ТЗ № 11
S: Система охранно-тревожной сигнализации предназначена для
а) постановки и снятия с охраны помещений;
б) формирования и выдачи сигналов тревоги при несанкционированном появлении или попытке проникновения человека в закрытые и сданные под охрану помещения;
в) просмотра состояния охраняемых помещений на планах в графической форме на автоматизированных рабочих местах и отображения на них сигналов тревоги или неисправности;
-:Верны только варианты а,б
-:Верны только варианты б,в
+:Верны все варианты

I: ТЗ № 12
S: Система обеспечения безопасности включает в себя (4 верных ответа)
+:Систему охранно-тревожной сигнализации
-: Систему медицинского мониторинга служащих.
+:Систему контроля и управления доступом
+:Систему пожарной сигнализации
+:Систему периметровой охраны
-: Систему оповещения населения об опасности.

I: ТЗ № 13
S: Обеспечение безопасности объекта базируется на следующих принципах (два верных ответа)
+:определение и оценка угроз объекту;
-: поиск угроз за пределами предприятия.
+:разработка и реализация адекватных мер защиты.

Тема 2. Краткая характеристика основных способов защиты объектов.
I: ТЗ № 1
S: Акустические извещатели – это
+:извещатели, формирующие сигнал тревоги при регистрации в охраняемой зоне характерного звука, например, звука разбивания оконного стекла.
-: извещатели, формирующие сигнал тревоги при скачкообразном падении атмосферного давления в охраняемом помещении, которое может произойти в случае открытия двери или окна.
-: извещатели, которые сочетают в себе два или более физических принципа действия.

I: ТЗ № 2
S: Сейсмические извещатели – это
+: извещатели, устанавливаемые на жесткую конструкцию и формирующие сигнал тревоги в случае регистрации в этой конструкции колебаний, возникающих при попытке разрушения преграды.

-:извещатели, излучающие ультразвуковые колебания и принимающие сигнал, отраженный от окружающих предметов. Формирование тревожного сигнала происходит в случае возникновения движения в контролируемой зоне.
-: извещатели, излучающие в диапазоне ультракоротких радиоволн.

I: ТЗ № 3
S: Пьезоэлектрические извещатели – это
+: различные извещатели, использующие в своей работе материалы, которые обладают свойством наведения разности потенциалов на противоположных сторонах кристалла при его деформации.
-: извещатели, формирующие сигнал тревоги при размыкании геркона вследствие удаления от него магнитного элемента. Устанавливаются как правило на окна и входные двери.
-: извещатели, формирующие сигнал тревоги при скачкообразном падении атмосферного давления в охраняемом помещении, которое может произойти в случае открытия двери или окна.

I: ТЗ № 4
S: По физическому принципу действия извещатели можно подразделить на следующие группы.
+: Магнитоконтактные, электроконтактные, комбинированные
-: морские, речные, сухопутные
-:ручные, автоматические, релейные

I: ТЗ № 5
S: Магнитоконтактные извещатели – это
+: извещатели, формирующие сигнал тревоги при размыкании геркона вследствие удаления от него магнитного элемента. Устанавливаются как правило на окна и входные двери.
-: извещатели, формирующие сигнал тревоги при скачкообразном падении атмосферного давления в охраняемом помещении, которое может произойти в случае открытия двери или окна.
-: различные извещатели, использующие в своей работе материалы, которые обладают свойством наведения разности потенциалов на противоположных сторонах пьезоэлектрического кристалла при его деформации.

I: ТЗ № 6
S: Электроконтактные извещатели – это
+: извещатели, которые формируют сигнал тревоги при размыкании электрического контакта. В настоящее время используются как правило в системах тревожной сигнализации и работают в ручном режиме.
-: извещатели, формирующие сигнал тревоги при размыкании геркона вследствие удаления от него магнитного элемента. Устанавливаются как правило на окна и входные двери.
-: извещатели, формирующие сигнал тревоги при скачкообразном падении атмосферного давления в охраняемом помещении, которое может произойти в случае открытия двери или окна.

I: ТЗ № 7
S: Комбинированные извещатели – это
+: -: извещатели, которые сочетают в себе два или более физических принципа действия (инфракрасный и ультразвуковой, инфракрасный и радиоволновой).

-: извещатели, которые формируют сигнал тревоги при размыкании электрического контакта. В настоящее время используются как правило в системах тревожной сигнализации и работают в ручном режиме.
-: извещатели, формирующие сигнал тревоги при размыкании геркона вследствие удаления от него магнитного элемента. Устанавливаются как правило на окна и входные двери.

I: ТЗ № 8
S: Система контроля и управления доступом предназначена для
+: выполнения комплекса мероприятий, направленных на ограничение и санкционирование доступа сотрудников на территорию предприятия, в помещения и зоны ограниченного доступа.
-: выполнения комплекса мероприятий, направленных на беспрепятственный проход сотрудников на территорию предприятия, в помещения и зоны ограниченного доступа.
-: выполнения комплекса мероприятий, направленных блокирование сотрудников при попытке проникновения на территорию предприятия, в помещения и зоны ограниченного доступа.

I: ТЗ № 9
S: Система контроля и управления доступом обеспечивает:
а) интеграцию с другими системами ИСБ на программно-аппаратном уровне;
б) многоуровневую организацию доступа с возможностью корректировки базы данных администратором ИСБ в соответствии с решаемыми задачами;
в) возможность графического отображения состояния системы (наличие тревог, нештатных ситуаций, оперативной информации с выводом поэтажных планов, мест установки технических средств системы КУД);
г) создание архива с объемом памяти, обеспечивающим регистрацию всех фактов посещения предприятия сотрудниками и посетителями с указанием даты и времени посещения, их фотографий и иных данных с возможностью хранения и использования в течение одного года;
-:Верны только варианты а,б
-:Верны только варианты б,в
-:Верны только варианты а,г
+:Верны все варианты

I: ТЗ № 10
S: Система контроля и управления доступом обеспечивает:
а) интеграцию с другими системами ИСБ на программно-аппаратном уровне;
б) многоуровневую организацию доступа с возможностью корректировки базы данных администратором ИСБ в соответствии с решаемыми задачами;
в) возможность графического отображения состояния системы (наличие тревог, нештатных ситуаций, оперативной информации с выводом поэтажных планов, мест установки технических средств системы КУД);
г) создание архива с объемом памяти, обеспечивающим регистрацию всех фактов посещения предприятия сотрудниками и посетителями с указанием даты и времени посещения, их фотографий и иных данных с возможностью хранения и использования в течение одного года;
-:Верны только варианты а,б
-:Верны только варианты б,в
-:Верны только варианты а,г
+:Верны все варианты

I: ТЗ № 11
S: Система контроля и управления доступом обеспечивает:
а) создание архива с объемом памяти, обеспечивающим регистрацию всех фактов посещения предприятия сотрудниками и посетителями с указанием даты и времени посещения, их фотографий и иных данных с возможностью хранения и использования в течение одного года;
б) возможность ежедневного архивирования базы данных разовых посетителей в конце рабочего дня, ведение протоколов, электронных журналов;
в) возможность перехода на ручное управление отдельными элементами СКУД с защитой паролем и подтверждением дежурным службы безопасности с автоматическим протоколированием данного факта;
г) возможность развития за счет расширения программно-аппаратных частей без нарушения работоспособности смонтированного оборудования, а также возможность модернизации в случае изменения или расширения функций (задач), выполняемых системой.
-:Верны только варианты а,б
-:Верны только варианты б,в
-:Верны только варианты а,г
+:Верны все варианты

I: ТЗ № 12
S: Система контроля и управления доступом электронной проходной обеспечивает:
а) санкционированный доступ (вход и выход) сотрудников на территорию предприятия (основанием санкционированного доступа является карта-пропуск);
б) вывод фотоизображения сотрудников, имеющих постоянные и временные пропуска на мониторе оператора поста охраны на КПП;
в) возможность блокирования выхода через проходные в случае поступления сигнала тревоги;
г) компьютерный учет входа и выхода посетителей и сотрудников с ведением протокола в компьютере и выводом протокола на принтер.
-:Верны только варианты а, б
-:Верны только варианты б, в
-:Верны только варианты б-г
+:Верны все варианты

I: ТЗ № 13
S: Управление проходами через турникеты может осуществляться 3 верных ответа)
+: в автоматическом режиме
-: в приоритетном режиме
+: полуавтоматическом режиме
-: в избирательном режиме
+: ручном режиме

I: ТЗ № 14
S: На АРМах может быть реализован
+:режим фотоидентификации
-: режим видеоидентификации
-: режим тестирования

I: ТЗ № 15
S: Для ручного управления турникетами на рабочем месте устанавливаются специальные
+:кнопочные панели

-: тактильные системы
-:фотоаппараты

Тема 3. Системы сбора, обработки информации (ССОИ).
I: ТЗ № 1
S: СКУД обеспечивает (2 верных ответа):
+: контроль и регистрацию перемещения сотрудников в протоколе компьютера;
-: выход с территории предприятия в случае аварийной ситуации
+:аварийную разблокировку дверей с поста охраны центрального входа.

I: ТЗ № 2
S: СКУД обеспечивает:
+:санкционированный доступ сотрудников в зоны, выделенные помещения и кабинеты согласно разграничению прав доступа;
-: несанкционированный доступ сотрудников в зоны, выделенные помещения и кабинеты;

I: ТЗ № 3
S: СКУД обеспечивает (2 верных ответа):
+:выдачу сигнала тревоги на АРМ СКУД в случае несанкционированного проникновения в зоны доступа и выделенные помещения (вскрытие двери) или в случае не закрытия двери;
-:проход на территорию предприятия экскурсантов
+:компьютерный учет входа и выхода посетителей и сотрудников с ведением протокола в компьютере и выводом протокола на принтер;

I: ТЗ № 4
S: Телевизионные системы широко применяются для
+:наблюдения за территорией охраняемого объекта или за обстановкой внутри помещения.
-:поиска неработающих сотрудников предприятия

I: ТЗ № 5
S: Телевизионные системы имеют общую структуру, в составе которой
+:несколько передающих ТВ-камер подключаются к центральному пульту, где устанавливаются один или несколько мониторов
-:одна телевизионная камера
-:несколько фотоаппаратов

I: ТЗ № 6
S: Телевизионная система предназначена для (2 верных ответа):
+:усиления охраны и внутриобъектового режима на охраняемом объекте;
-:контроля загруженности работников предприятия
+:организации технологического наблюдения в местах установки системы пожаротушения.

I: ТЗ № 7
S: Телевизионная система обеспечивает (2 верных ответа):
+:контроль выполнения технологических процессов внутри помещений объекта,
-:контроль в местах отдыха сотрудников охраны
+:контроль государственных номеров автотранспорта, подъезжающего к внешним воротам транспортных КПП

I: ТЗ № 8
S: Телевизионная система обеспечивает (2 верных ответа):
+:контроль выполнения технологических процессов внутри помещений объекта,
+:контроль зоны досмотра транспортных средств,
-:контроль государственных номеров автотранспорта, проезжающего возле транспортных КПП

I: ТЗ № 9
S: Телевизионная система обеспечивает (2 верных ответа):
-:контроль выполнения санитарной обработки внутри помещений объекта,
+:контроль зоны досмотра транспортных средств,
+:контроль государственных номеров автотранспорта, подъезжающего к внешним воротам транспортных КПП

I: ТЗ № 10
S: При разработке систем телевизионного наблюдения (СТН) учитываются следующие основные требования (3 верных ответа):
+:возможность создания единой системы видеонаблюдения со сквозной нумерацией всех камер и единой базой данных о конфигурации системы;
-:возможность просмотра телевизионных программ
+:возможность расширения общего количества видеокамер;
+:наличие на АРМ постов охраны тревожных телевизионных мониторов

I: ТЗ № 11
S: При разработке систем телевизионного наблюдения (СТН) учитываются следующие основные требования (3 верных ответа):
-:возможность трансляции программ спутникового телевидения
+:возможность интеграции СТН в комплекс инженерно-технических средств охраны;
+:возможность расширения общего количества видеокамер;
+:наличие на АРМ постов охраны тревожных телевизионных мониторов

I: ТЗ № 12
S: При разработке систем телевизионного наблюдения (СТН) учитываются следующие основные требования (3 верных ответа):
+:возможность создания единой системы видеонаблюдения со сквозной нумерацией всех камер и единой базой данных о конфигурации системы;
+:возможность интеграции СТН в комплекс инженерно-технических средств охраны;
-:возможность уменьшения общего количества видеокамер;
+:наличие на АРМ постов охраны тревожных телевизионных мониторов

I: ТЗ № 13
S: Система пожарной сигнализации (ПС) предназначена для (3 верных ответа):
+:выдачи адресного сообщение об обнаружении очага возгорания в помещение поста охраны с указанием адреса датчика
-:вызова городской пожарной команды
+:выдачи сообщение «неисправность» в помещение поста охраны с указанием адреса датчика;
+:выдачи сигнала «пожар» на систему оповещения людей о пожаре, запуске системы для блокирования приточной вентиляции и на другие системы;

I: ТЗ № 14
S: Система пожарной сигнализации (ПС) предназначена для (3 верных ответа):

-:выдачи сигналов об эвакуации персонала предприятия
+:управления установками автоматического пожаротушения;
+:фиксации факта и времени обнаружении очага возгорания, и отображения информации в реальном масштабе времени на мониторах АРМов операторов ИСБ;
-:отключения электропитания
+:ведения электронного журнала, фиксирующего действия операторов в стандартных и нештатных ситуациях.

I: ТЗ № 15
S: Система пожарной сигнализации (ПС) предназначена для (3 верных ответа):
+:выдачи сигнала «пожар» на систему оповещения людей о пожаре, запуске системы для блокирования приточной вентиляции и на другие системы;
+:управления установками автоматического пожаротушения;
+:фиксации факта и времени обнаружении очага возгорания, и отображения информации в реальном масштабе времени на мониторах АРМов операторов ИСБ;
-:ведения протокола о действиях сотрудников предприятия в экстремальной ситуации

I: ТЗ № 16
S: Система пожарной сигнализации (ПС) предназначена для (3 верных ответа):
-:ведения протокола о поведении сотрудников предприятия в экстремальной ситуации
+:фиксации факта и времени обнаружении очага возгорания, и отображения информации в реальном масштабе времени на мониторах АРМов операторов ИСБ;
+:ведения протокола событий системы ПС в памяти компьютера с возможностью просмотра на мониторе и его распечатки;
-:отключения электричества
+:ведения электронного журнала, фиксирующего действия операторов в стандартных и нештатных ситуациях.

I: ТЗ № 17
S: Модуль порошкового пожаротушения предназначен для (3 верных ответа)
+:тушения и локализации пожаров твердых материалов,
+:тушения и локализации пожаров горючих жидкостей
+:тушения и локализации пожаров электрооборудования до 5000 В
-:для тушения щелочных металлов,

I: ТЗ № 18
S: Модуль порошкового пожаротушения предназначен для (3 верных ответа)
+:тушения и локализации пожаров твердых материалов,
+:тушения и локализации пожаров горючих жидкостей
+:тушения и локализации пожаров электрооборудования до 5000 В
-:для тушения щелочноземельных металлов,

I: ТЗ № 19
S: Модуль порошкового пожаротушения предназначен для (3 верных ответа)
+:тушения лесных пожаров,
+:тушения и локализации пожаров горючих жидкостей
+:тушения и локализации пожаров электрооборудования до 5000 В
-:для тушения щелочных и щелочноземельных металлов,

I: ТЗ № 20
S: В основе работы оптического дымового извещателя лежит принцип
+:рассеивания света

-: фокусирования света
-:преобразования длины волны света

Тема 4. Системы контроля и управления доступом.
I: ТЗ № 1
S: При создании периметровой охраны объекта особой важности его внутренняя территория (охраняемая площадь) должна быть условно разделена на несколько функциональных зон (2 верных ответа):
-:отдыха
+:наблюдения
-:тренировок
+:поражения

I: ТЗ № 2
S: При создании периметровой охраны объекта особой важности его внутренняя территория (охраняемая площадь) должна быть условно разделена на несколько функциональных зон (3 верных ответа):
+:обнаружения
+:поиска
+:поражения
-: нулевой видимости

I: ТЗ № 3
S: При создании периметровой охраны объекта особой важности его внутренняя территория (охраняемая площадь) должна быть условно разделена на несколько функциональных зон (3 верных ответа):
+:обнаружения
+:наблюдения
-:предупреждения
+:поражения

I: ТЗ № 4
S: Зона обнаружения (ЗО) – зона, в которой непосредственно располагаются
+:периметровые средства обнаружения, выполняющие автоматическое обнаружение нарушителя и выдачу сигнала «Тревога»
-: инженерные заграждения, создающие физические препятствия перемещению злоумышленника

I: ТЗ № 5
S: Зона наблюдения (ЗН) предназначена
+:для слежения с помощью технических средств (телевидение, радиолокация и т.д.) за обстановкой на подступах к границам охраняемой зоны и в ее пространстве
-:для задержания злоумышленника
-: задержания нарушителя

I: ТЗ № 6
S: Зона физического сдерживания (ЗФС) представляет собой (3 верных ответа)
+:различные виды заборов,
-:всевозможные вооружения
+:спирали из колючей ленты и проволоки,
-:груды камней
+:механические задерживающие преграды

I: ТЗ № 7
S: Зона физического сдерживания (ЗФС) представляет собой (3 верных ответа)
-:рекламные плакаты
+:козырьки,
+:спирали из колючей ленты и проволоки,
-:предупреждающие надписи
+:механические задерживающие преграды

I: ТЗ № 8
S: Зона физического сдерживания (ЗФС) представляет собой (2 верных ответа)
+:различные виды заборов,
-: предупреждающие надписи
+:стенды

I: ТЗ № 9
S: Зона средств физической нейтрализации и поражения (ЗНП) предназначена для –
а) нейтрализации злоумышленников.
б) поражения злоумышленников
-: оба ответа неправильные
+: оба ответа верные

I: ТЗ № 10
S: Зона физической нейтрализации и поражения (ЗНП) располагается
В зоне обнаружения
В зоне физического сдерживания
-: оба ответа неправильные
+: оба ответа верные

I: ТЗ № 11
S: В зоне физической нейтрализации и поражения помещаются средства физического воздействия, которые подразделяются на (2 верных ответа)
-:ударные,
+:ограничивающие возможность свободного перемещения (быстро застывающая пена),
+:огнестрельное оружие, минные поля и т.п.

I: ТЗ № 12
S: В зоне физической нейтрализации и поражения помещаются средства физического воздействия, которые подразделяются на
а) электрошоковые,
б) ослепляющие (вспышки),
в) оглушающие,
г) удушающие,
д) ограничивающие возможность свободного перемещения (быстро застывающая пена), средства нейтрализации и поражения – огнестрельное оружие, минные поля и т. п.
-:Верны только варианты а-в
-:Верны только варианты в-г
-:Верны только варианты б-д
+:Верны все варианты

I: ТЗ № 13

S: В зоне физической нейтрализации и поражения помещаются средства физического воздействия, которые подразделяются на
а) электрошоковые,
б) успокаивающие
в) оглушающие,
г) возбуждающие
д) ограничивающие возможность свободного перемещения (быстро застывающая пена), средства нейтрализации и поражения – огнестрельное оружие, минные поля и т.п.
-:Верны только варианты а-в
-:Верны только варианты в-г
-:Верны только варианты б-д
+:Верны все варианты

I: ТЗ № 14
S: Система телевизионного наблюдения имеет структуру -
-: две передающие ТВ-камеры подключенные к центральному пульту
+: несколько передающих ТВ-камер подключаются к центральному пульту, где устанавливаются один или несколько мониторов, на которые можно выводить изображение от любой из передающих камер
-: одна передающая ТВ-камера не подключенная к центральному пульту

I: ТЗ № 15
S: Система телевизионного наблюдения (СТН) предназначена для (2 верных ответа):
+: усиления охраны и внутриобъектового режима на охраняемом объекте;
-: контроля за порядком на объекте
+: организации технологического наблюдения в местах установки системы пожаротушения.

I: ТЗ № 16
S: Система телевизионного наблюдения (СТН) обеспечивает (3 верных ответа):
+: интеграцию с другими системами ИСБ на программно-аппаратном уровне;
+: визуальный контроль периметра предприятия, контроль выполнения технологических процессов внутри помещений объекта, контроль зоны досмотра транспортных средств, контроль государственных номеров автотранспорта, подъезжающего к внешним воротам транспортных КПП;
+: получение должностными лицами дежурного персонала службы безопасности видеоинформации с телевизионных камер в соответствии с настройками системы
-: получение тактильной и звуковой информации

I: ТЗ № 17
S: Система телевизионного наблюдения (СТН) обеспечивает (4 верных ответа)
+: получение должностными лицами дежурного персонала производственных подразделений объекта видеоинформации с телевизионных камер;
-: порядок на объекте
+: приоритетное включение каналов для просмотра и запись при срабатывании технических средств систем безопасности в зоне наблюдения телекамер;
+: круглосуточную запись изображений со всех видеокамер с последующей возможностью воспроизведения;
+: работоспособное состояние при прекращении электроснабжения в течение не менее 1 ч.
-: получение тактильной и звуковой информации

I: ТЗ № 18
S: При разработке систем телевизионного наблюдения (СТН) учитываются следующие основные требования (4 верных ответа):
+: возможность создания единой системы видеонаблюдения со сквозной нумерацией всех камер и единой базой данных о конфигурации системы;
+: возможность интеграции СТН в комплекс инженерно-технических средств охраны;
-:возможность установки светочувствительных детекторов
+:возможность расширения общего количества видеокамер;
+: наличие на АРМ постов охраны тревожных телевизионных мониторов, вывод изображений на которые возможен в автоматическом режиме по сигналам от технических средств других систем, входящих в интегрированную систему безопасности (ИСБ)
-:возможность установки тепловых детекторов

I: ТЗ № 19
S: При разработке систем телевизионного наблюдения (СТН) учитываются следующие основные требования (3 верных ответа):
+: обеспечение скорости записи не менее 7 кадров в секунду по каждой камере при максимальном качестве изображения;
-:возможность установки тепловых детекторов
+: оперативное видеоархивирование в течение не менее одной недели в непрерывном режиме записи с использованием современных средств хранения информации с возможностью поиска и просмотра видеофрагментов по нескольким параметрам: дате, времени и событиям;
-:возможность установки светочувствительных детекторов
+: возможность передачи оцифрованного видеокадра или видеосюжета по локальной сети, распечатки видеокадра на принтере, а также записи видеокадров/ видеосюжетов на CD или другие стандартные переносные носители.

I: ТЗ № 20
S: Способы установки видеокамер (2 верных ответа)
+:устанавливается стационарно
-:устанавливаются на передвижных платформах
+:использование поворотного устройства с трансфокаторными объективами.

Тема 5. Системы охранно-пожарной сигнализации.
I: ТЗ № 1
S: Видеосигналы и сигналы управления от телевизионных камер транслируются на (3 верных ответа)
+:зональный узел по волоконнооптической линии связи
+: по кабельным линиям связи.
+: по локальной вычислительной сети (ЛВС) предприятия.
-: по глобальной вычислительной сети

I: ТЗ № 2
S: Выберите неправильное утверждение. Черно-белые телекамеры
-: стоят в полтора раза дешевле цветных,
-: разрешающая способность у них выше в полтора-два раза
-: чувствительность выше в 4–8 раз
-: применяют при наблюдении больших открытых территорий.
+: в настоящее время не применяются

I: ТЗ № 3

S: Система пожарной сигнализации (ПС) предназначена для (3 верных ответа):
+: выдачи адресного сообщение об обнаружении очага возгорания в помещение поста охраны с указанием адреса датчика (для каждого датчика в отдельности задается уровень чувствительности для выдачи сообщения «внимание» и «пожар», раздельно для дневного и ночного режимов);
+: выдачи сообщение «неисправность» в помещение поста охраны с указанием адреса датчика;
-: выдачи сигнала «всем оставаться на своих местах» на систему оповещения людей о пожаре
+: выдачи сигнала «пожар» на систему оповещения людей о пожаре, пускатели системы для блокирования приточной вентиляции и на другие системы;
-: выдачи сигнала на пускатели системы для деблокирования приточной вентиляции и на другие системы

I: ТЗ № 4
S: Система пожарной сигнализации (ПС) предназначена для (3 верных ответа):
+: управления установками автоматического пожаротушения;
+: возможности работы в автономном режиме с выполнением вышеуказанных требований;
-: выдачи сигнала «всем оставаться на своих местах» на систему оповещения людей о пожаре
+: фиксацию факта и времени обнаружении очага возгорания, и отображение информации в реальном масштабе времени на мониторах АРМов операторов ИСБ;
-: выдачи сигнала на пускатели системы для деблокирования приточной вентиляции и на другие системы

I: ТЗ № 5
S: Система пожарной сигнализации (ПС) предназначена для (3 верных ответа):
+: ведение протокола событий системы ПС в памяти компьютера с возможностью просмотра на мониторе и его распечатки;
-: выдачи сигнала на пускатели системы для деблокирования приточной вентиляции и на другие системы
+: ведение электронного журнала, фиксирующего действия операторов в стандартных и нештатных ситуациях;
+: выдачи адресного сообщение об обнаружении очага возгорания в помещение поста охраны с указанием адреса датчика (для каждого датчика в отдельности задается уровень чувствительности для выдачи сообщения «внимание» и «пожар», раздельно для дневного и ночного режимов);

I: ТЗ № 6
S: Системой автоматического пожаротушения оборудуются
+:кабельные туннели
-:воздушные линии электропитания
-: водные линии электропитания

I: ТЗ № 7
S: Управление системой пожаротушения производится при помощи
+:специализированных сетевых контроллеров
-:специализированных процессоров
-:специализированных регистров

I: ТЗ № 8

S: Модуль порошкового пожаротушения предназначен для
+:тушения и локализации пожаров твердых материалов, горючих жидкостей и электрооборудования до 5000 В в производственных, складских, бытовых и других помещениях.
-: тушения и локализации пожаров щелочных металлов

I: ТЗ № 9
S: Тушению не подлежат (2 верных ответа)
+: щелочные и щелочноземельные металлы,
+: вещества, горение которых может происходить без воздуха.
-: все химические вещества, находящиеся на складе

I: ТЗ № 10
S: Адресно-аналоговые пожарные извещатели
+: измеряют уровень задымленности, температуру в помещении и передают эту информацию на приёмно-контрольную панель
-: определяют задымленность
-: измеряют температуру

I: ТЗ № 11
S: Основное отличие адресно-аналоговых пожарных извещателей от адресных и традиционных пороговых систем является, то что адресно-аналоговые пожарные извещатели
+: измеряют уровень задымленности, температуру в помещении и передают эту информацию на приёмно-контрольную панель
-: определяют задымленность
-: измеряют температуру
-: фиксируют влажность и атмосферное давление

I: ТЗ № 12
S: В качестве базового извещателя применяют оптико-электронный дымовой извещатель. В основе его работы лежит принцип
+: рассеивания света.
-: определения задымленности
-: измерения температуры
-: фиксации влажности

I: ТЗ № 13
S: Осуществление мероприятий по обеспечению превентивной и адекватной безопасности населения и промышленных объектов представляет собой
+: сложный непрерывный процесс,
-: одноразовые, случайные действия, которые выполняются от случая к случаю по мере возникновения опасности
-: квартальные, полугодовые, ежегодные проверки

I: ТЗ № 14
S:Непрерывное и стабильное функционирование любого объекта невозможно без организации надежной защиты, включающей в себя:
+:комплекс мер, направленных на выявление основных угроз и опасных ситуаций, оценки ущерба при осуществлении этих угроз, создания системы комплексной безопасности объекта

-: комплекс мер, направленных на выявление недобросовестных работников

I: ТЗ № 15
S:Безопасность защищаемого объекта – это
а) состояние защищенности объекта от угроз причинения ущерба (вреда) жизни или здоровью людей;
б) имуществу физических или юридических лиц; в) государственному или муниципальному имуществу;
г) техническому состоянию, инфраструктуре жизнеобеспечения; д) внешнему виду, интерьеру, ландшафтной архитектуре, окружающей природной среде.
-:Верны только а, б
-:Верны только б,г
+:Верны все ответы

I: ТЗ № 16
S:Для организации эффективной защиты необходимо разработать обобщенную системную концепцию безопасности, которая в каждом конкретном случае должна быть адаптирована
+: к конкретному объекту, исходя из условий его функционирования, расположения, характера деятельности, географического положения, особенностей окружающей среды и прочих факторов.
-: к любым объектам, независимо от условий его функционирования, расположения, характера деятельности, географического положения, особенностей окружающей среды и прочих факторов.

I: ТЗ № 17
S: Концепция обеспечения комплексной безопасности объекта предназначена для решения следующих задач (верны 3 ответа):
+: определение целей или предметов защиты, иначе, "кого или что защищать?" (объект – квартира, офис, предприятие);
+: определение и оценка угроз, иначе, "от какого посягательства защищать?" (случайный хулиган, рецидивист или организованная группа);
-: разработка и реализация максимальных мер защиты независимо от степени угрозы
+: разработка и реализация адекватных мер защиты, иначе, "чем и как защищать?" (что должна сделать охранная система, чтобы предотвратить или уменьшить ущерб).

I: ТЗ № 18
S:Уязвимость объекта – это
+:степень несоответствия принятых мер по защите объекта прогнозируемым угрозам или заданным требованиям безопасности.
-: степень возможного поражения и разрушения объекта при воздействии на него чрезвычайных ситуаций техногенного характера
-: степень возможного поражения и разрушения объекта при воздействии на него чрезвычайных ситуаций природного характера

I: ТЗ № 19
S: Целями и задачами проведения анализа уязвимости являются:
а) определение важных для жизнедеятельности объекта предметов защиты;
б) определение возможных угроз и моделей вероятных исполнителей угроз;
в) оценка возможного ущерба от реализации прогнозируемых угроз безопасности
-:Верны только а, б
-:Верны только б,в

+:Верны все ответы

I: ТЗ № 20
S: Целями и задачами проведения анализа уязвимости являются:
а) оценка уязвимости объекта и существующей системы безопасности;
б) разработка общих рекомендаций по обеспечению безопасности объекта.
в) определение важных для жизнедеятельности объекта предметов защиты;
-:Верны только а, б
-:Верны только б,в
+:Верны все ответы

Тема 6. Интегрированные системы безопасности.

I: ТЗ № 1
S: Классификация предметов защиты и объектов охраны. Охраняемый объект – это
а) предприятие, организация, жилище, их часть или комбинация, оборудованные действующей системой охраны и безопасности.
б) объект, охраняемый подразделениями охраны и оборудованный действующими техническими средствами охранной, пожарной и т.д.
в) здания, строения, сооружения, прилегающие к ним территории и акватории, транспортные средства, а также грузы, в том числе при их транспортировке
-:Верны только а, б
-:Верны только б,в
+:Верны все ответы

I: ТЗ № 2
S: Для промышленного предприятия важными предметами защиты являются (2 верных ответа):
+: люди (персонал предприятия);
+:имущество: важное или дефицитное технологическое оборудование;
-:служащие охраны
-:имущество руководства предприятия

I: ТЗ № 3
S: Для промышленного предприятия важными предметами защиты являются (2 верных ответа):
+: секретная и конфиденциальная документация;
-:служащие охраны
-:имущество руководства предприятия
+: материальные и финансовые ценности;

I: ТЗ № 4
S: Для промышленного предприятия важными предметами защиты являются (3 верных ответа):
+: готовая продукция;
-:имущество руководства предприятия
+: интеллектуальная собственность (ноу-хау);
+: средства вычислительной техники;

I: ТЗ № 5
S: Для промышленного предприятия важными предметами защиты являются (2 верных ответа):

+: контрольно-измерительные приборы и др.;
-:служащие охраны
+: информация конфиденциальная (на материальных носителях, а также циркулирующая во внутренних коммуникационных каналах связи и информации, в кабинетах руководства предприятия, на совещаниях и заседаниях);

I: ТЗ № 6
S: Утрата перечисленных ресурсов ведет к следующим событиям (3 верных ответа):
+: значительному материальному ущербу;
+: созданию угрозы для жизни и здоровья людей;
+: разглашению конфиденциальной информации или сведений, содержащих государственную или коммерческую тайну; банкротству предприятия.
-:краху государственных структур

I: ТЗ № 7
S: Что необходимо защищать на стационарных и подвижных объектах:
а) здания, строения, сооружения, их отдельные части или помещения;
б) территории, занимаемые ими, или прилегающие к ним, отдельные территории, отдельные предметы;
в) транспортные средства (автомобильный, железнодорожный,
водный, воздушный транспорт).
д)имущество руководства предприятия
+:Только ответы а-в
-:Только ответы в, д
-:Все ответы верны

I: ТЗ № 8
S: К инженерным средствам защиты объектов НЕ относятся
-:различные заборы, ограждения, решетки, жалюзи, ставни, замки, засовы,
-:укрепленные двери, ворота, стены, полы, потолки, оконные проемы, воздуховоды
+: компьютерные защитные средства

I: ТЗ № 9
S: Инженерно-техническая укрепленность объекта – это
+:совокупность мероприятий, направленных на усиление конструктивных элементов зданий, сооружений, помещений и защищаемых территорий
-:совокупность мероприятий, направленных на компьютерные защитные средства.
-:совокупность мероприятий, направленных на видео контроль территории

I: ТЗ № 10
S: Требования к инженерно-технической укрепленности объекта защиты формулируются с учетом его
а) категории,
б) строительными решениями
в) архитектурно-планировочными решениями,
г) режимом работы объекта.
-:Только ответы а-в
-:Только ответы в, д
+:Все ответы верны

I: ТЗ № 11

S: Объекты группы AI
а) объекты особо важные, повышенной опасности и жизнеобеспечения, включенные в Перечень объектов, подлежащих государственной охране; б) объекты по производству, хранению и реализации наркотических веществ, сильнодействующих ядов и химикатов, токсичных и психотропных веществ и препаратов;
в) ювелирные магазины, базы, склады и другие объекты, использующие в своей деятельности ювелирные изделия, драгоценные металлы и камни;
-:Только ответы а,б
-:Только ответы б,в
+:Все ответы верны

I: ТЗ № 12
S: Объекты группы AI
а) объекты и помещения для хранения оружия и боеприпасов, радиоизотопных веществ и препаратов,
б) предметов старины, искусства и культуры;
в) объекты кредитно-финансовой системы (банки, операционные кассы вне кассового узла, дополнительные офисы, пункты обмена валюты, банкоматы)
-:Только ответы а,б
-:Только ответы б,в
+:Все ответы верны

I: ТЗ № 13
S: Объекты группы AI
а) кассы предприятий, организаций, учреждений, головные кассы крупных торговых предприятий;
б) сейфовые комнаты, предназначенные для хранения денежных средств, ювелирных изделий, драгоценных металлов и камней;
в) другие аналогичные объекты и имущественные комплексы.
-:Только ответы а,б
-:Только ответы б,в
+:Все ответы верны

I: ТЗ № 14
S: Объекты группы AII:
а) хранилища и кладовые денежных и валютных средств, ценных бумаг;
б) хранилища ювелирных изделий, драгоценных металлов и камней;
в) хранилища секретной документации, изделий;
-:Только ответы а,б
-:Только ответы б,в
+:Все ответы верны

I: ТЗ № 15
S: Объекты группы AII:
а) хранилища секретной документации, изделий;
б) специальные хранилища взрывчатых, наркотических, ядовитых, бактериологических, токсичных и психотропных веществ и препаратов;
в) специальные фондохранилища музеев и библиотек.
-:Только ответы а,б
-:Только ответы б,в
+:Все ответы верны

Тема 7. Системы теленаблюдения.
I: ТЗ № 1
S: Объекты группы АII:
а) хранилища секретной документации, изделий;
б) специальные хранилища взрывчатых, наркотических, ядовитых, бактериологических, токсичных и психотропных веществ и препаратов;
в) специальные фондохранилища музеев и библиотек.
-:Только ответы а,б
-:Только ответы б,в
+:Все ответы верны

I: ТЗ № 2
S: Объекты группы БI (2 верных ответа):
+: объекты с хранением или размещением изделий технологического, санитарно-гигиенического и хозяйственного назначения, нормативно-технической документации, инвентаря и другого имущества;
+: объекты мелкооптовой и розничной торговли (павильоны, палатки, ларьки, киоски и другие аналогичные объекты).
-: хранилища секретной документации, изделий;
-: кассы предприятий, организаций, учреждений

I: ТЗ № 3
S: Объекты группы БII – это объекты с хранением или размещением
+: предметов повседневного спроса, продуктов питания,
+: компьютерной техники, оргтехники, видео- и аудиотехники, кино- и фотоаппаратуры,
+: натуральных и искусственных мехов, кожи,
+: автомобилей и запасных частей к ним,
-: хранилища и кладовые денежных и валютных средств, ценных бумаг;

I: ТЗ № 4
S: Класс защиты конструктивных элементов АI, АII, БI, БII. Регламентируется соответствие характеристик элементов
-: Минимальная, средняя, высокая, специальная степень защиты объекта
+: Специальная, высокая, средняя, минимальная степень защиты объекта
-: Супервысокая, высокая, низкая степень защиты объекта

I: ТЗ № 5
S: В зависимости от степени потенциальной опасности и возможных последствий в случае реализации криминальных угроз объекты подразделяются на три основные группы:
+: критически важные и потенциально опасные объекты;
+: социально значимые объекты;
+: объекты сосредоточения материальных ценностей.
-: социально незначимые объекты;

I: ТЗ № 6
S: Источниками угрозы безопасности могут выступать (3 верных ответа)
+: человек,
+: техногенная среда
+: природа
-: животные
-: космические частицы

I: ТЗ № 7
S: К основным угрозам безопасности можно отнести (3 верных ответа):
+: угрозы жизни, здоровью, личным правам и свободам человека;
+: угрозы материальным и культурным ценностям;
+:угрозы физическим носителям информации;
-: угрозы общественной деятельности человека

I: ТЗ № 8
S: К основным угрозам безопасности можно отнести (3 верных ответа):
+: угрозы экономической деятельности;
-: угрозы политической деятельности
+: угрозы общественной безопасности;
+: угрозы информационной безопасности;

I: ТЗ № 9
S: Безопасность защищаемого объекта должна быть комплексной для решения следующих важных задач (3 верных ответа):
+: поддержание безопасного состояния объекта;
-: поддержание чистоты
+: предупреждение угроз;
+: обнаружение угроз;

I: ТЗ № 10
S: Безопасность защищаемого объекта должна быть комплексной для решения следующих важных задач (2 верных ответа):
-: поддержание порядка
+: противодействие угрозам;
+: ликвидация последствий максимального количества из полного набора возможных угроз для данного объекта.

Тема 8. Выбор средств видеоконтроля для оборудования объектов, особенности их эксплуатации.
I: ТЗ № 1
S: Непрерывное и стабильное функционирование любого объекта невозможно без организации надежной защиты, включающей в себя комплекс мер, направленных на (3 верных ответа)
+: выявление основных угроз и опасных ситуаций,
+: оценки ущерба при осуществлении этих угроз,
+: создания системы комплексной безопасности объекта при определенных ограничениях (например, на стоимость системы).
-: поддержание чистоты и порядка на предприятии

I: ТЗ № 2
S: Безопасность защищаемого объекта – это состояние защищенности объекта от угроз причинения (3 верных ответа)
+: ущерба (вреда) жизни или здоровью людей;
+: имуществу физических или юридических лиц;
+: государственному или муниципальному имуществу;
-:порядку на объекте

I: ТЗ № 3
S: Уязвимость (объекта) – это степень несоответствия принятых мер по защите объекта прогнозируемым угрозам или заданным требованиям безопасности. Целями и задачами проведения анализа уязвимости являются (3 верных ответа):
а) определение важных для жизнедеятельности объекта предметов защиты (наиболее вероятных целей злоумышленных акций нарушителей);
б) оценка уязвимости объекта и существующей системы безопасности;
в) разработка общих рекомендаций по обеспечению безопасности
объекта.
-:Верны только варианты а,б
-:Верны только варианты б,в
+:Верны все варианты

I: ТЗ № 4
S: Для промышленного предприятия важными для жизнедеятельности предметами защиты являются:
а) люди (персонал предприятия);
б) имущество:
в) важное или дефицитное технологическое оборудование;
-:Только ответы а,б
-:Только ответы б,в
+:Все ответы верны

I: ТЗ № 5
S: Для промышленного предприятия важными для жизнедеятельности предметами защиты являются (3 верных ответа):
+: секретная и конфиденциальная документация;
+: материальные и финансовые ценности;
+: готовая продукция;
-:слесарные инструменты

I: ТЗ № 6
S: Для промышленного предприятия важными для жизнедеятельности предметами защиты являются (3 верных ответа):
+: интеллектуальная собственность (ноу-хау);
-:столярные инструменты
+: интеллектуальная собственность (ноу-хау);
+: средства вычислительной техники;

I: ТЗ № 7
S: Утрата перечисленных ресурсов ведет к следующим событиям:
а) значительному материальному ущербу;
б) созданию угрозы для жизни и здоровья людей;
в) разглашению конфиденциальной информации или сведений, содержащих Государственную или коммерческую тайну;
г) банкротству предприятия.
-:Только ответы а,б
-:Только ответы б,в
+:Все ответы верны

I: ТЗ № 8
S: В связи с широким спектром угрожающих факторов безопасность защищаемого объекта должна быть комплексной для решения следующих важных задач (3 верных ответа):
+: поддержание безопасного состояния объекта;
-: поддержание чистоты и порядка на объекте
+: предупреждение угроз;
+: обнаружение угроз;

I: ТЗ № 9
S: В связи с широким спектром угрожающих факторов безопасность защищаемого объекта должна быть комплексной для решения следующих важных задач (3 верных ответа):
+: противодействие угрозам;
+: ликвидация последствий максимального количества из полного набора возможных угроз для данного объекта.
+: угрозы жизни, здоровью, личным правам и свободам человека;
-:угрозы личному имуществу граждан

I: ТЗ № 10
S: Система охранно-тревожной сигнализации обеспечивает:
а) паролирование и иерархическое распределение доступа сотрудников к функциям и регламентам системы;
б) работоспособное состояние при прекращении электроснабжения – в течение не менее 4 часов;
в) возможность независимой работы в случае нарушения связи с сервером или выхода из строя компьютерной техники
-:Верны только варианты а,б
-:Верны только варианты б, в
-:Верны только варианты а,в
+:Верны все варианты

I: ТЗ № 11
S: Охранные инфракрасные извещатели – это
+:извещатели, которые обнаруживают тепловое излучение человеческого тела и формируют сигнал тревоги в случае, когда источник теплового излучения движется.
-:извещатели, излучающие ультразвуковые колебания и принимающие сигнал, отраженный от окружающих предметов.
-: извещатели, излучающие в диапазоне ультракоротких радиоволн.

I: ТЗ № 12
S: Охранные ультразвуковые извещатели – это
+: извещатели, излучающие колебания и принимающие сигнал, отраженный от окружающих предметов. Формирование тревожного сигнала происходит в случае возникновения движения в контролируемой зоне.
-: извещатели, излучающие в диапазоне ультракоротких радиоволн.
-:извещатели, которые обнаруживают тепловое излучение человеческого тела и формируют сигнал тревоги в случае, когда источник теплового излучения движется.

I: ТЗ № 13
S: По физическому принципу действия извещатели можно подразделить на следующие группы.

+:Инфракрасные, ультразвуковые ,радиоволновые, барометрические
-: морские, речные, сухопутные
-:ручные, автоматические, релейные

I: ТЗ № 14
S: По физическому принципу действия извещатели можно подразделить на следующие группы.
+:Акустические, сейсмические, инерционные, пьезоэлектрические
-: морские, речные, сухопутные
-:ручные, автоматические, релейные

I: ТЗ № 15
S: Барометрические извещатели – это
+: извещатели, формирующие сигнал тревоги при скачкообразном падении атмосферного давления в охраняемом помещении, которое может произойти в случае открытия двери или окна.
-: извещатели, которые сочетают в себе два или более физических принципа действия.
-:извещатели, излучающие ультразвуковые колебания и принимающие сигнал, отраженный от окружающих предметов. Формирование тревожного сигнала происходит в случае возникновения движения в контролируемой зоне.

I: ТЗ № 16
S: Инерционные извещатели – это
+: извещатели, в которых сигнал тревоги формируется при механическом воздействии на охраняемый объект, например, автомобиль (покачивание, толчки).
-: извещатели, излучающие в диапазоне ультракоротких радиоволн.
-:извещатели, которые обнаруживают тепловое излучение человеческого тела и формируют сигнал тревоги в случае, когда источник теплового излучения движется.

I: ТЗ № 17
S: Можно выделить основные типы извещателей (два верных ответа):
+: Пассивные извещатели, которые сами не являются источниками волн различной физической природы
+: Активные извещатели, являющиеся источниками волн.
-: Нейтральные извещатели

1.2 Оценочные материалы для промежуточной аттестации

Зачет проводится по билетам. В каждом билете 3 теоретических вопроса. Задачи для промежуточной аттестации берутся из банка задач, приведенных в оценочных материалах текущего контроля, случайным образом.

Вопросы к зачету

1. Исходные положения для разработки концепции обеспечения безопасности объектов.
2. Категории объектов охраны. Требования к технической укрепленности объектов.
3. «Модель» нарушителя. Пути и способы его проникновения на охраняемый объект.
4. Инженерные средства защиты. Технические средства охраны, в том числе электронные средства: средства обнаружения, средства коммуникации.
5. ССОИ - аппаратно-центральная система обеспечения взаимодействия человека с комплексом технических средств.
6. Классификация функции ССОИ в составе комплексов технических средств охраны. Структура построения ССОИ.
7. Пластиковые карточки, карточки со штрих-кодом, карточки с магнитной полосой, смарт-карты. Аудиодомофонные устройства. Видеодомофонные устройства.
8. Системы контроля доступа. Физические средства защиты.
9. Системы охранно-пожарной сигнализации. Извещатели. Приемно-контрольные приборы.
10. Системы охранно-пожарной сигнализации. Системы передачи сообщений. Резервные источники питания.
11. Системы охранно-пожарной сигнализации. Пожарная сигнализация.
12. Структура и функции интегрированной системы охраны. Выбор характеристик ИСО для конкретного объекта.
13. Интегрированная система охраны. Назначение системы. Функции системы.
14. Рекомендации по интерфейсу RS-485. Удлинение линии интерфейса RS-485 с помощью модемов.
15. Системы теленаблюдения. Особенности применения систем видеонаблюдения.
16. Противопожарные средства охраны. Основные требования для ОПС. Компоненты систем ОПС.
17. Извещатели охранной и пожарной сигнализации.
18. Извещатели, основанные на разных принципах действия.
19. Виды помех и их возможные источники.
20. Принцип выбора пожарных извещателей для защиты объекта.
21. Определение интегрированной системы охраны. Общие требования и принципы организации.
22. Структура и функции интегрированной системы охраны. Выбор характеристик ИСО для конкретного объекта.
23. Назначение, классификация и состав систем контроля и управления доступом.
24. Устройства идентификации (считыватели)
25. Биометрические средства идентфикации личности
26. Варианты реализации систем контроля и управления доступом
27. Автономные, сетевые и распределенные контроллеры
28. Физические средства защиты. Системы контроля доступа.
29. Структура и функции интегрированной системы охраны. Выбор характеристик ИСО для конкретного объекта.
30. Телевизионные камеры и устройства для их оснащения. Многофункциональные матричные коммутаторы системы видеонаблюдения.

31. Цифровые системы видеонаблюдения: алгоритмы сжатия видео изображения.
32. Выбор телевизионной камеры. Скрытое наблюдение. Требования к аппаратуре постов управления и каналов передачи видеосигнала. Расчет устройства видеонаблюдения.