Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия промышленных технологий»

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по выполнению практических работ

МДК.03.02 Инженерно-технические средства физической защиты объектов информации

для специальности
среднего профессионального образования

10.02.05 Обеспечение информационной безопасности автоматизированных систем

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 3
ПРАВИЛА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ 5
ОПИСАНИЕ РАБОЧЕГО МЕСТА ОБУЧАЮЩЕГОСЯ 5
ПРАКТИЧЕСКИЕ РАБОТЫ 6
- Практическая работа № 1 6
- Практическая работа № 2 10
- Практическая работа № 3 11
- Практическая работа № 4 14
- Практическая работа № 5 16
- Практическая работа № 6 17
- Практическая работа № 7 18
- Практическая работа № 8 19
- Практическая работа № 9 21
- Практическая работа № 10 22

ВВЕДЕНИЕ

Место дисциплины в основной образовательной программе: МДК.03.02 Инженерно-технические средства физической защиты объектов информации является обязательным разделом профессионального модуля ПМ.03 «Защита информации техническими средствами» основной образовательной программы по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Формируемые МДК.03.02 «Инженерно-технические средства физической защиты объектов информации» компетенции, знания, умения:

Знания

- порядок технического обслуживания технических средств защиты информации;
- номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;
- физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;
- порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;
- методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;
- номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;
- основные принципы действия и характеристики технических средств физической защиты;
- основные способы физической защиты объектов информатизации;
- номенклатуру применяемых средств физической защиты объектов информатизации.

Умения

- применять технические средства для криптографической защиты информации конфиденциального характера;
- применять технические средства для уничтожения информации и носителей информации;
- применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;
- применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;
- применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;
- применять инженерно-технические средства физической защиты объектов информатизации

Профессиональные компетенции

ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.

ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.

ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.

ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.

Общие компетенции

ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.

ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.

ОК 9. Использовать информационные технологии в профессиональной деятельности.

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.

Методические указания предназначены для проведения практических занятий по МДК.03.02, закрепления теоретических знаний и получения навыков работы в области инженерно-технических средств защиты информации.

Методические указания разработаны в соответствии с рабочей программой профессионального модуля ПМ.03 «Защита информации техническими средствами» по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем»

Методические указания включают 10 практических работ. Каждая практическая работа содержит сведения о теме, цели ее проведения и формируемых компетенциях, включает пояснения к работе, содержание отчета, контрольные задания или вопросы.

К выполнению практических работ обучаемые приступают после подробного изучения соответствующего теоретического материала и прохождения инструктажа по технике безопасности.

ПРАВИЛА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

Практические работы выполняются в лаборатории Технических средств защиты информации.

Перед выполнением практической работы необходимо повторить теоретический материал по соответствующей теме.

К самостоятельной работе обучающиеся допускаются только после инструктажа по технике безопасности и пожарной безопасности.

После выполнения практической работы обучающиеся приводят в порядок рабочее место, показывают преподавателю полученные результаты. После утверждения преподавателем предъявленных результатов, каждый обучающийся оформляет отчет о проделанной работе, представляет его на проверку преподавателю в тот же день или на следующем практическом занятии.

ОПИСАНИЕ РАБОЧЕГО МЕСТА ОБУЧАЮЩЕГОСЯ

1. Практические работы выполняются в лаборатории Технических средств защиты информации.
2. Для выполнения практических работ используется следующее оборудование:
   - Персональный компьютер;
   - Виртуальный тренажёр "Аттестация объекта по требованиям защиты от утечек информации по техническим каналам" (лицензия на 1 рабочее место), ТЗИ-ВИРТ-СРТФ;
   - Учебный стенд системы видеонаблюдения;
   - Учебный стенд СКУД.

ПРАКТИЧЕСКИЕ РАБОТЫ

Практическая работа № 1

Тема: Характеристика объекта защиты

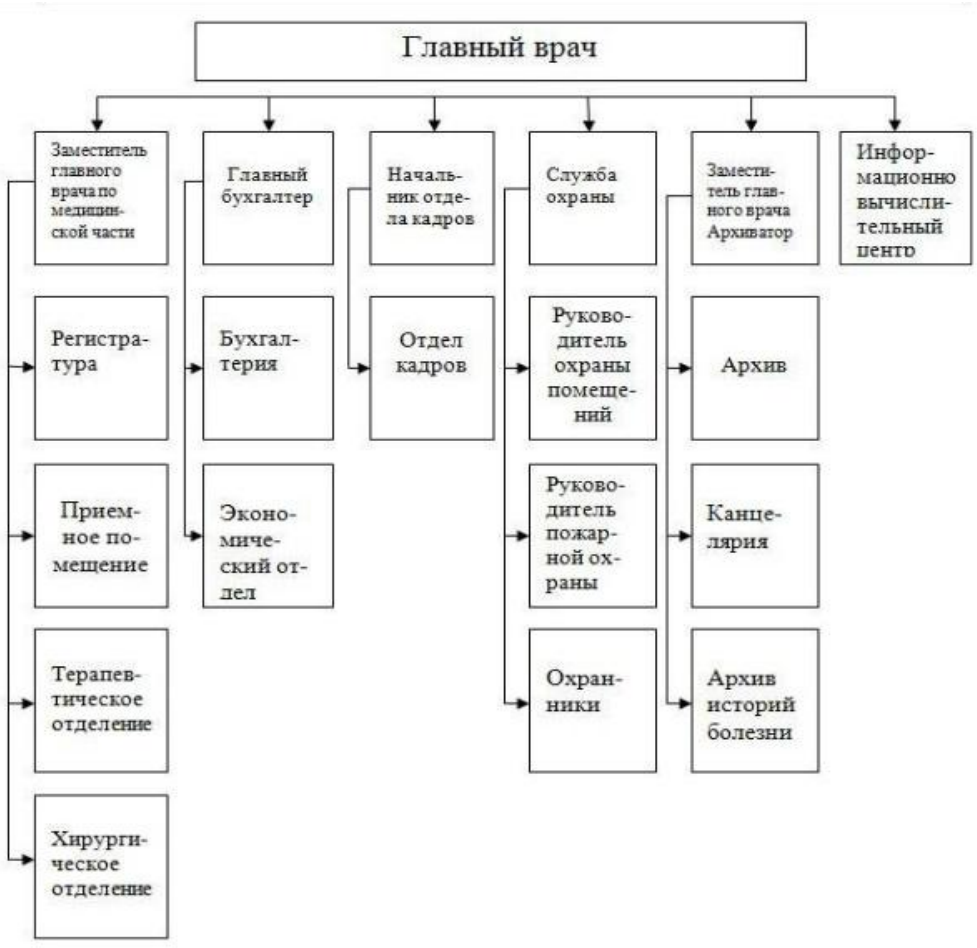
Цель: анализ структуры, деятельности и защищаемых ресурсов объекта, категорирование объекта защиты.

Формируемые компетенции: ПК 3.5, ОК 01, ОК 02, ОК 04, ОК 05, ОК 09, ОК 10.

Задание 1.

Построение структуры подразделений объекта защиты, характеристика назначения объекта и решаемых задач. Определение функционально-отраслевой принадлежности объекта.

Структура подразделений объекта может быть представлена в виде схемы или таблицы. Под организационной структурой предприятия понимаются состав, соподчиненность, взаимодействие и распределение работ по подразделениям и органам управления, между которыми устанавливаются определенные отношения по поводу реализации властных полномочий, потоков команд и информации. Организационная структура объекта построена по линейно-функциональному признаку. Пример организационной структуры объекта (поликлиники):



Далее необходимо перечислить решаемые задачи и направления деятельности, осуществляемой на объекте. Привести описание ведущихся на объекте работ, дать характеристику операций, выполняемых на объекте, и условий их выполнения. Сформулировать назначение объекта.

Определить, к какому типу относится заданный объект. Определить виды и масштабы возможного ущерба в результате нарушения безопасности. Определить категорию заданного объекта по уровню важности в соответствии с ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) «Системы тревожной сигнализации».

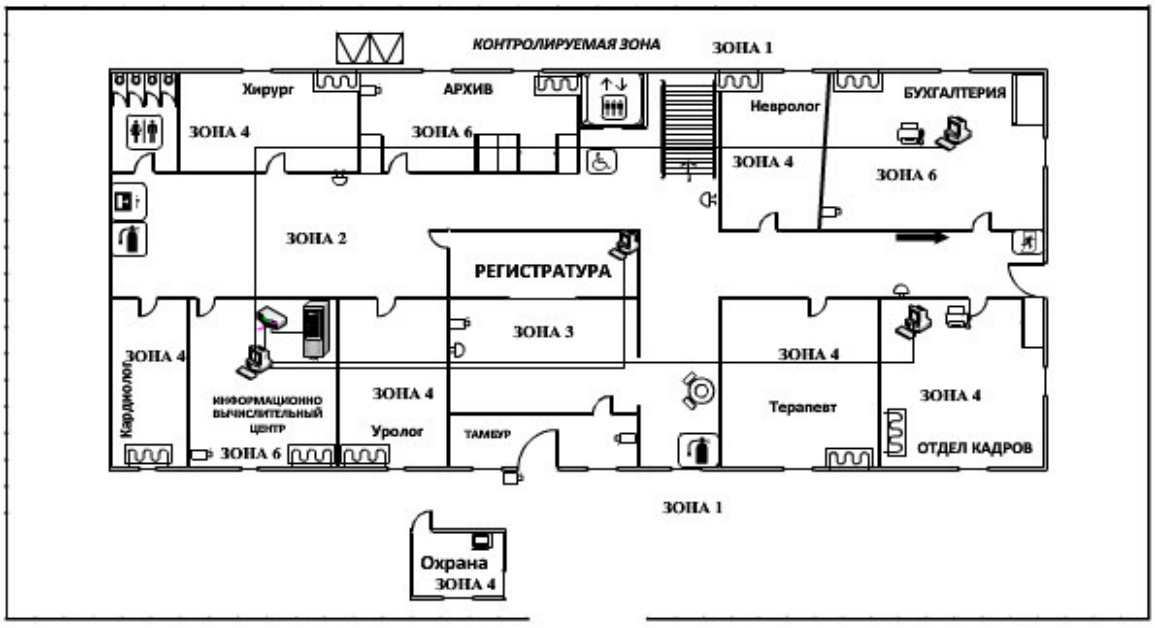
Задание 2.

Определение содержания и местонахождения защищаемых ресурсов на объекте, например:

Объект защиты	Место расположения
Персонал, пациенты	Основное здание больницы и прилегающая к ней территория
Здания, сооружения	Территория предприятия
Конфиденциальная информация	Регистратура, кабинеты больницы
Носители конфиденциальной информации: документы, содержащие ПДн, служебную и коммерческую информацию	Основное здание больницы (кабинеты 5,6,3)
Оборудование и медтехника	Кабинеты 3,4
Средства вычислительной техники	Кабинеты 3,4,5,6
Финансовые ценности	Кабинет руководителя (кабинет 2)
Фармацевтические препараты	Аптека больницы

Задание 3.

Построить план объекта, с помощью принятых стандартом условных обозначений показать все объекты защиты. Определить категории защищаемых зон. Определить структуру контролируемых зон. Пример плана объекта:



Определить категории контролируемых зон, заполнить таблицу по данным исследуемого объекта защиты:

Категория	Наименование зоны	Функциональное назначение зоны	Условия доступа сотрудников	Условия доступа посетителей	Наличие охраны
I	Свободная		Свободный	Свободный	Есть
II	Наблюдаемая		Свободный	Свободный	Есть
III	Регистрационная		Свободный	Свободный с регистрацией по удостоверениям личности	Есть
IV	Режимная		По служебн. удостоверениям или идентификационным картам	По разовым пропускам	Усиленная охрана
V	Усиленной защиты		По спецдокументам	По спецпропускам	Усиленная охрана
VI	Высшей защиты		По спецдокументам	По спецпропускам	Усиленная охрана

Задание 4.

Характеристика технической укрепленности объекта. Построение пространственной модели объекта защиты. Проанализировать характеристики технической укрепленности объекта защиты, заполнить таблицу:

Наименование параметра	Данные
1	2
Площадь, кв.м	
Высота потолка, м	
Толщина стен: наружных, внутренних, м	
Окна: количество, размер	
Двери: размер проема, тип замков	
Описание смежных помещений: сверху, сбоку слева, сбоку справа, снизу	
Система электропитания (освещение): тип светильников и их количество	
Система заземления	
Системы сигнализации	
Система вентиляции (тип)	
Наличие экранов на батареях	
Телефонные линии: городская сеть, тип розеток	

Построение пространственной модели объекта защиты. Провести анализ месторасположения объекта (в какой части города расположен объект), какие объекты находятся в ближайшем окружении. Составить пространственную модель объекта:

Пространственная характеристика помещения	Функциональная, конструктивная и техническая характеристика помещения		
Этаж	2	Площадь, $м^2$	56
Количество окон, тип сигнализации, наличие штор на окнах			
Двери, кол-во, одинарные, двойные			
Соседские помещения, названия, толщина стен			

Задание 6.

Определение категории защищаемого объекта. В результате выполнения задач были определены функционально-отраслевая принадлежность исследуемого объекта, виды и масштабы возможного ущерба в результате нарушения безопасности, категория важности защищаемой информации на объекте.

Кроме названных характеристик необходимо определить пожаро- и взрывоопасность данного объекта, что осуществляется в соответствии с Федеральным законом № 117-ФЗ от 10 июля 2012 г. «Технический регламент о требованиях пожарной безопасности». Результаты решения поставленной задачи занести в таблицу:

Информативный признак категории	Категория наследуемого объекта
По функционально-отраслевой принадлежности	
По виду возможного ущерба	
По масштабу возможного ущерба	
По важности объекта	
По категории информации	
По пожаро- и взрывоопасности	

По численности персонала свыше 500 человек	
По материальным активам свыше 500 МРОТ	

Варианты объектов физической защиты:

№ варианта	Объект информатизации
1	Здание администрации завода железобетонных изделий
2	Здание торгового центра
3	Здание поликлиники
4	Корпус университета
5	Здание научно-производственного объединения
6	Здание фармацевтической фирмы
7	Здание районного отдела полиции
8	Здание банка
9	Здание патентного бюро
10	Здание редакции научного издания
11	Здание научно-исследовательского института
12	Здание склада текстильной продукции
13	Здание рекламного агентства
14	Здание производственных цехов бурового оборудования
15	Здание птицефабрики
16	Здание республиканской библиотеки
17	Здание музея изобразительных искусств
18	Здание школы
19	Здание больницы
20	Здание районного суда

Содержание отчета:

1. Организационная структура объекта защиты.
2. Перечень мест расположения защищаемых ресурсов.
3. План объекта защиты
4. Перечень категорий контролируемых зон объекта защиты.
5. Характеристики технической укрепленности объекта защиты.
6. Пространственная модель объекта.
7. Структурная модель конфиденциальной информации.
8. Выводы о категории защищаемого объекта.

Контрольные вопросы:

1. Сущность и задачи физической защиты объектов информатизации.
2. Анализ структуры физической защиты.
3. Принципы физической защиты объектов информатизации.
4. Методы физической защиты объектов информатизации.
5. Схема анализа защищаемого объекта информатизации.
6. Категорирование защищаемой информации.
7. Анализ возможных источников угроз безопасности.

Практическая работа № 2

Тема: Формирование требований к физической защите объекта. Анализ нормативно-правовой базы физической защиты**.**

Цель: формирование требований к физической защите на основе анализа нормативно-правовых документов и характеристики объекта.

Формируемые компетенции: ПК 3.1. ПК 3.2, ПК 3.5, ОК 01, ОК 02, ОК 04, ОК 05, ОК 06, ОК 09, ОК 10

Задание 1.

Изучить нормативно-правовые документы по физической защите объектов. Сформировать таблицу внешних и внутренних документов. Для заданного объекта в результате выполнения практической работы № 15 были выявлены такие характеристики, как категория важности объекта, категории защищаемой информации, категория объекта по взрыво- и пожароопасности, по виду и масштабу ущерба. Для реализации эффективной физической защиты объекта необходимо сформировать требования, которые предъявляют нормативно-правовые документы к объекту полученной категории.

Все нормативно-правовые документы можно разделить на 2 группы: руководящие документы федерального значения и отраслевые или внутренние документы, разработанные непосредственно для заданного объекта. Заполнить таблицу:

Уровень документа	Наименование документа	Краткое пояснение
1	2	3
Федеральные		
Внутренние		

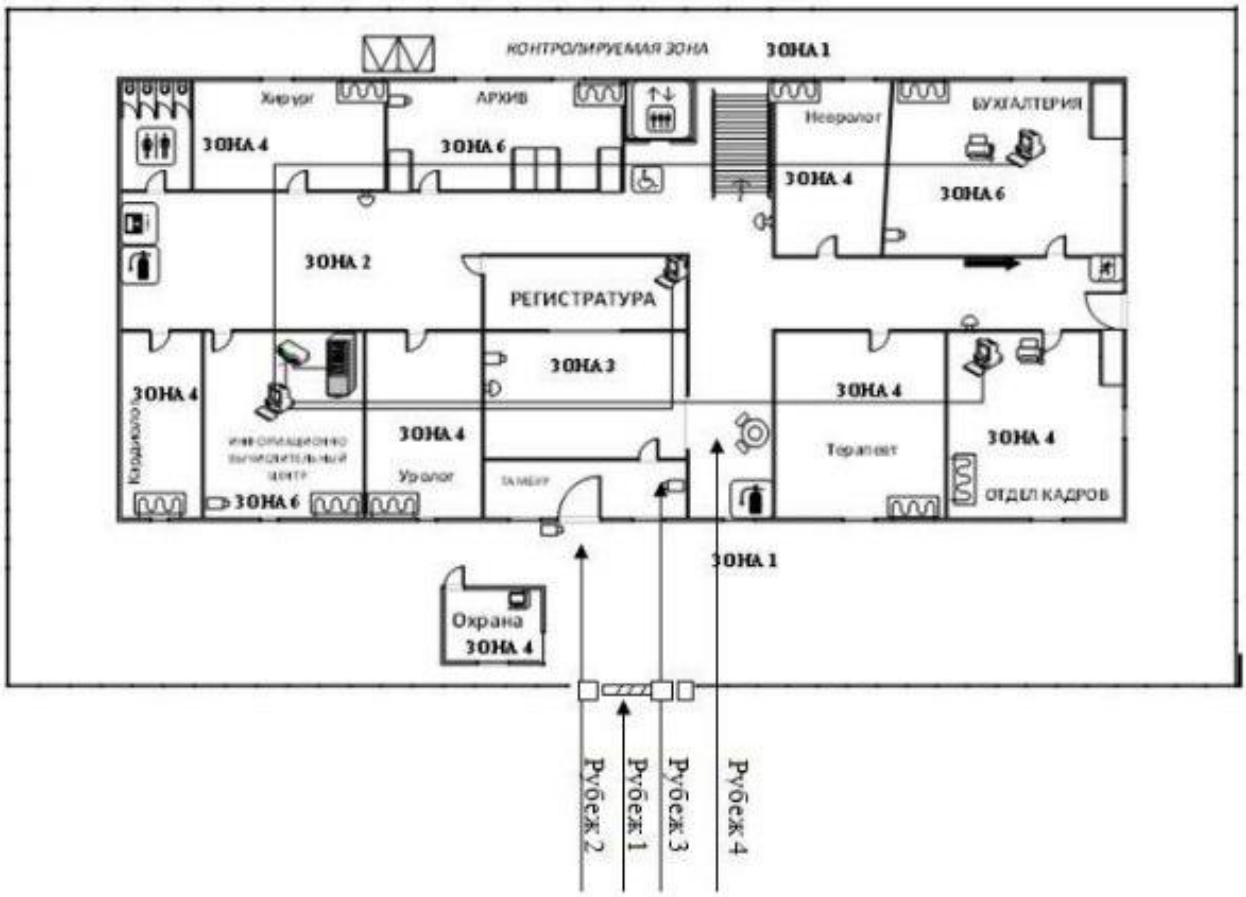
Задание 2.

Сформировать перечень требований к системе физической защиты заданного объекта. В соответствии с полученными данными обследования объекта составить таблицы требований к физическим средствам защиты заданного объекта информатизации в соответствии с РД 78.36.003-2002 «Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств» по следующим пунктам:

- количество рубежей защиты объекта;
- класс защиты конструктивных элементов (строительные конструкции, дверные, оконные конструкции);
- класс защиты основного ограждения;
- класс защиты ворот;
- характеристики дверных конструкций;
- класс защиты запирающих устройств;
- типы извещателей для обнаружения криминального воздействия;
- наличие системы контроля доступа;
- характеристики системы видеонаблюдения;
- характеристики системы охранного освещения;
- характеристики системы оповещения.

Задание 3.

Определить количество рубежей защиты для заданного объекта, построить схему рубежей с пояснениями. Пример построения рубежей:



Содержание отчета

1. Перечень внешних и внутренних угроз для защищаемого объекта
2. Перечень нормативно-правовых документов, устанавливающих требования к защите выбранного объекта
3. Требования к физическим средствам защиты выбранного объекта информатизации
4. Схема рубежей защиты

Контрольные вопросы

1. Нормативно-правовые документы по физической защите объектов.
2. Перечень требований к системе физической защиты заданного объекта.

Практическая работа № 3

Тема: Монтаж датчиков пожарной и охранной сигнализации

Цель: формирование подсистемы обнаружения нарушителя безопасности.

Формируемые компетенции: ПК 3.1, ПК 3.2, ПК 3.5, ОК 01-10

Задание 1.

Провести выбор и обоснование охранных извещателей.

Факторы, влияющие на выбор средств обнаружения, по вариантам указаны в таблице Виды растительности: Н – низкая (кустарник), С – средняя (высокие кусты акации, сирени и т.д.), В – высокая (деревья).

№ варианта, фактор	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Наличие полосы отчуждения	+	-	-	-	-	-	-	-	-	-	-	+	-	-	+	-
Особенности рельефа	-	+	-	+	-	+	-	+	-	+	-	+	-	+	-	+

местности																
Наличие вблизи объекта ж/д	+	-	-	+	-	-	+	-	-	+	-	-	+	+	-	+
Наличие вблизи объекта линий электропередачи	-	+	+	-	+	+	-	+	+	-	+	+	-	-	+	-
Виды растительности	Н	Н	Н	С	С	В	С	В	Н	С	В	В	Н	Н	В	С
Трубопровод	-	+	-	-	-	-	+	-	+	-	-	+	-	-	-	+
Разрыв периметра для проезда транспорта, прохода людей	+	-	+	+	+	+	-	+	-	+	+	-	+	+	+	-

Выбор конкретного типа извещателя определяется в зависимости от:

- сопоставления конструктивных строительных характеристик объекта, подлежащего защите, и тактико-технических характеристик извещателя;
- характера и размещения ценностей в помещениях;
- помеховой обстановки на объекте;
- вероятных путей проникновения нарушителя;
- режима и тактики охраны.

Выбрать охранные извещатели, привести их характеристики и заполнить таблицу:

Вид охранного извещателя	Функция	Модель извещателя	Место установки	Кол-во	Фирма изготовителя
Магнитоконтактные					
Радиолучевой					
Акустический					

Задание 2.

Провести выбор и обоснование пожарных извещателей. В зависимости от назначения здания, где устанавливается система пожарной безопасности, применяются и определенные датчики. Например, для установки пожарной сигнализации в складском помещении большого метража применяются лучевые датчики. Для установки пожарной сигнализации в помещениях с большим количеством находящихся в нем людей (кинотеатры, театры, библиотеки и др.) лучше всего использовать дымовые датчики. Если мы имеем дело со складским помещением, в котором хранится, например, древесина или другие легко воспламеняющиеся природные материалы, рекомендовано применять датчики, которые реагируют на открытый огонь. Должны учитываться мельчайшие детали помещения, в котором происходит установка пожарной сигнализации. Поскольку тепловые датчики несколько инертны при срабатывании, предпочтительней использовать датчики дымовые. На рынке пожарного оборудования существуют также комбинированные датчики. Они предназначены для оповещения о пожаре при изменении двух параметров (температурном и дымовом).

Провести выбор пожарных извещателей в соответствии с категорией объекта. Привести характеристики выбранных извещателей. Заполнить таблицу:

Вид пожарного извещателя	Функция	Модель извещателя	Место установки	Кол-во	Фирма изготовителя
Дымовой оптиколэлектронный					
Газовый					
Пламени					

Задание 3.

Провести выбор средств оповещения. При определении типа системы оповещения и выборе оборудования для ее проектирования необходимо руководствоваться нормативными документами, утвержденными в установленном законом порядке. В первую очередь это НПБ 77-98 (Нормы пожарной безопасности), устанавливающие общие технические требования к техническим средствам оповещения и управления эвакуацией, и НПБ 104-03, устанавливающие требования пожарной безопасности к СОУЭ, а также их типы с определением перечня объектов, подлежащих оснащению такими системами.

Требования вышеуказанных норм при выборе оборудования и проектировании систем оповещения являются обязательными. Для значительной части небольших и средних объектов нормами пожарной безопасности определена установка СОУЭ первого и второго типов.

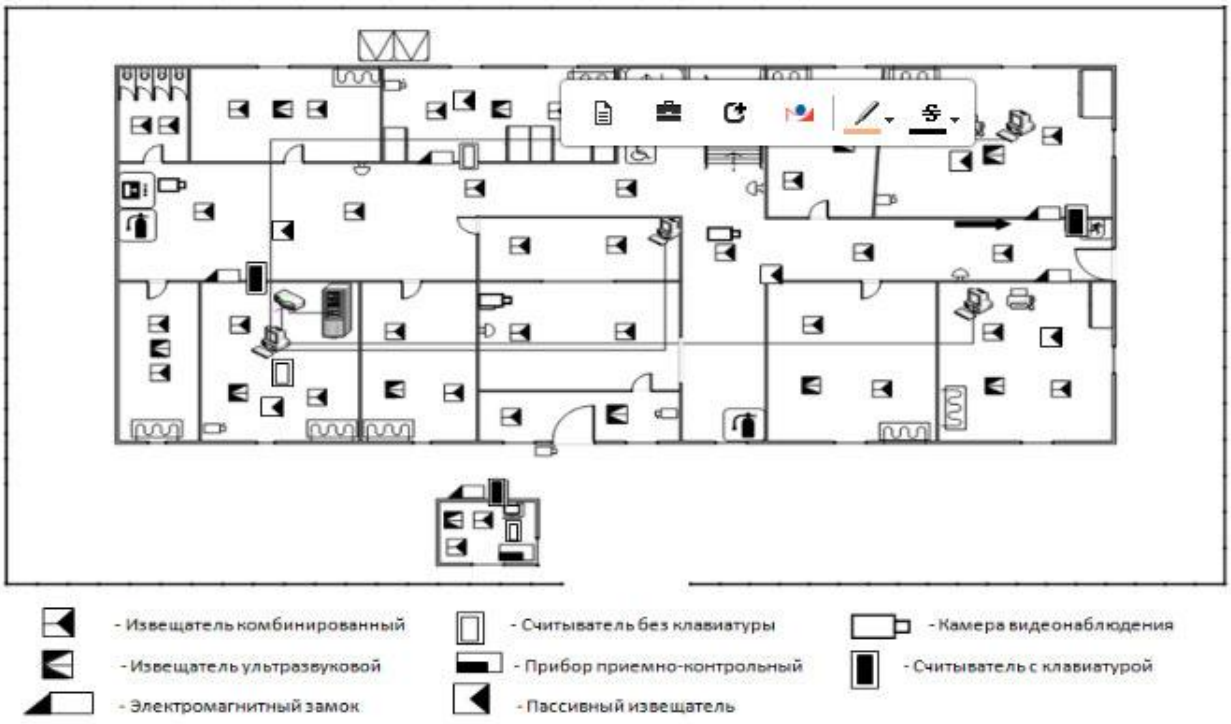
Для заданного объекта выбрать средства пожарного оповещения с учетом конкретных условий на объекте. Привести техническое описание выбранных средств оповещения. Классификация, общие технические требования и методы испытаний охранных оповещателей указаны в ГОСТ Р 54126-2010. Для заданного объекта выбрать тип охранных оповещателей. Привести характеристики выбранных средств оповещения.

Заполнить таблицу:

Вид оповещателя	Функция	Модель	Место установки	Кол-во	Фирма изготовителя
Речевой					
Звуковой					
Световой					

Задание 4.

Разработать схему размещения средств подсистемы обнаружения на объекте, например:



При разработке схемы расположения средств подсистемы обнаружения необходимо учитывать требования по геометрическим признакам помещений и территорий, а также технические характеристики приборов. Обозначения охранно-пожарного оборудования согласно требованиям рекомендаций РД 78.36.002-99 ГУВО МВД России. Технические средства систем безопасности объектов. Обозначения условные графические.

Содержание отчета

1. Таблица с характеристиками выбранных охранных извещателей
2. Таблица с характеристиками выбранных пожарных извещателей
3. Таблица с характеристиками выбранной системы оповещения
4. Схема размещения средств подсистемы обнаружения на объекте

Контрольные вопросы:

1. Пожарная связь и сигнализация.
2. Приемно-контрольные приборы пожарной и охранной сигнализации.
3. Интеграция охранно-пожарной сигнализации с комплексными системами безопасности здания.

Практическая работа № 4

Тема: Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя

Цель: изучить принципы устройства, работы и применения аппаратных средств аутентификации пользователя.

Формируемые компетенции: ПК 3.1, ПК 3.2, ПК 3.5, ОК 01 – 06, ОК 09, ОК 10.

Задание 1.

Приведите примеры программно-аппаратных систем аутентификации:

Задание 2.

Опишите назначение и возможности персонального средства аутентификации и хранения данных eToken.

Задание 3.

Приведите характеристики радиочастотных идентификаторов. Заполните таблицу:

Характеристика	Proximity	Смарт-карты	
		ISO/IEC 14443	ISO/IEC 15693
Частота радиоканала			
Дистанция чтения			
Встроенные типы чипов			
Функции памяти			
Ёмкость памяти			
Алгоритмы шифрования и			

аутентификации			
Механизм антиколлизии			

Задание 4.

Приведите характеристики USB-ключей. Заполните таблицу:

Изделие	Ёмкость памяти, кБ	Разрядность серийного номера	Алгоритмы шифрования
iKey 20xx			
eToken R2			
eToken Pro			
ePass 1000			
ePass 2000			
ruToken			
uaToken			

Задание 5.

Опишите функции комбинированных устройств аутентификации. Заполните таблицу:

Функция	Комбинированные системы		
	На базе бесконтактных смарт-карт и USB-ключей	На базе гибридных смарт-карт	Биоэлектронные системы
Идентификация и аутентификация компьютеров			
Блокировка работы компьютеров и разблокирование при предъявлении персонального идентификатора			
Идентификация и аутентификация сотрудников при их доступе в здание, помещение (из него)			
Хранение конфиденциальной информации (ключей шифрования, паролей, сертификатов и т.д.)			
Визуальная идентификация			

Содержание отчета

1. Описание персонального средства аутентификации и хранения данных eToken
2. Заполненная таблица характеристик радиочастотных идентификаторов
3. Заполненная таблица с характеристиками USB-ключей
4. Описание комбинированных устройств аутентификации

Контрольные вопросы:
1. Понятие аутентификации.
2. Способы аутентификации.
3. Аппаратные средства аутентификации.
4. Биометрические средства аутентификации.

Практическая работа № 5

Тема: Рассмотрение принципов устройства, работы и применения средств контроля доступа

Цель: изучить принципы устройства, работы и применения средств контроля доступа.

Формируемые компетенции: ПК 3.1, ПК 3.2, ПК 3.5, ОК 01 – 06, ОК 09, ОК 10

Задание 1.

Опишите основные компоненты системы контроля и управления доступом.

Задание 2.

Представьте характеристику карт пользователей:

Бесконтактные радиочастотные (PROXIMITY) карты	
Магнитные карты	
Карты Виганда	
Штрих-кодовые карты	

Задание 3.

Опишите назначение и возможности охранных панелей. Приведите исполнительные устройства охранных панелей.

Задание 4.

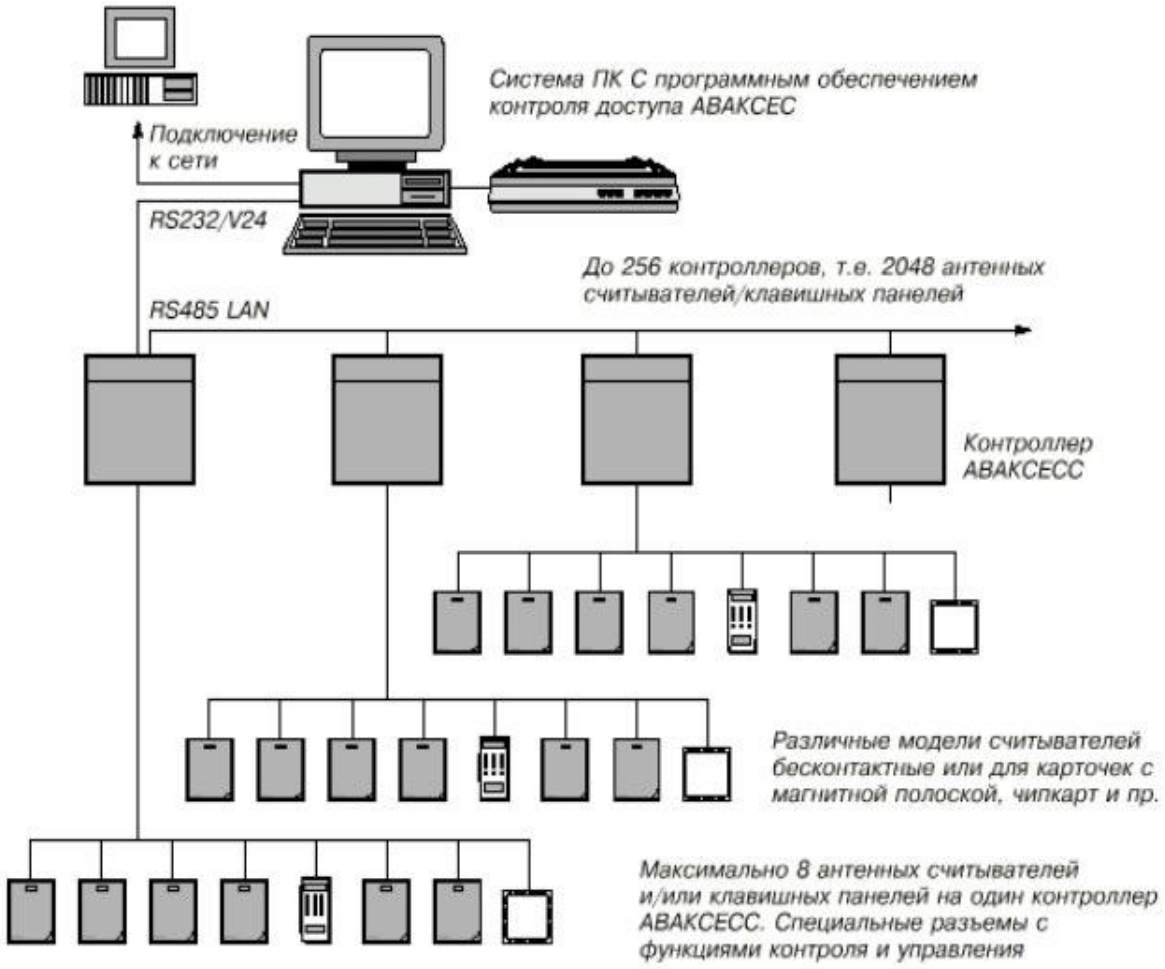
Опишите назначение и технологию управления шлюзами.

Задание 5.

Опишите технологию идентификации и регистрации транспортных средств антенным считывателем SmartPass.

Задание 6.

Опишите назначение системы АВАКСЕСС 500:



Содержание отчета

1. Описание принципов работы СКУД, различных пользовательских карт, шлюзов, антенного считывателя.

Контрольные вопросы:

1. Назначение систем контроля и управления доступом.
2. Структура систем контроля и управления доступом.
3. Направления развития систем контроля и управления доступом.

Практическая работа № 6

Тема: Рассмотрение принципов устройства, работы и применения средств видеонаблюдения

Цель: изучить принципы устройства, работы и применения средств видеонаблюдения.

Формируемые компетенции: ПК 3.1, ПК 3.2, ПК 3.5, ОК 01 – 06, ОК 09, ОК 10

Задание 1.

Опишите устройство и принципы работы IP-камеры:

Задание 2.

Приведите определения основных параметров видеокамеры:

Разрешение видеокамеры	
Светочувствительность	
Размер светочувствительной матрицы	
Отношение сигнал/шум	
Фокусное расстояние объектива	
Термический диапазон работы камеры	

Задание 3.

Опишите назначение и основные характеристики видеорегистраторов.

Задание 4.

Приведите характеристики сетевого видеорегистратора DVR.

Задание 5.

Приведите основные параметры видеомониторов.

Содержание отчета

1. Таблица с характеристиками видеокамеры
2. Сравнительная таблица видеорегистраторов

Контрольные вопросы:

1. Средства обработки видеоинформации.
2. IP-видеокамеры.
3. Основные параметры видеокамер.
4. Устройства видеозаписи.
5. Видеомониторы.
6. Устройства передачи видеосигналов.

Практическая работа № 7

Тема: Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации

Цель: изучить принципы устройства, работы и применения системы сбора и обработки информации.

Формируемые компетенции: ПК 3.1, ПК 3.2, ПК 3.5, ОК 01 – 06, ОК 09, ОК 10

Задание 1.

Опишите состав современных систем сбора и обработки информации. Приведите схему.

Задание 2.

Приведите алгоритмы расчета показателей надежности систем сбора и обработки информации:

- расчет оценки средней наработки на отказ;
- расчет оценки среднего времени восстановления;
- расчет оценки среднего времени реакции систем сбора и обработки информации на получение выходной информации по запросу;
- расчет оценки коэффициента готовности систем сбора и обработки информации.

Задание 3.

Опишите возможности системы сбора и обработки информации ОРИОН.

Содержание отчета

1. Структурная схема современных систем сбора и обработки информации
2. Результаты расчета показателей надежности системы сбора и обработки информации

Контрольные вопросы:

1. Комплекс технических средств обработки информации.
2. Получение первичной информации и регистрация.
3. Средства приема и передачи информации.
4. Средства обработки информации.
5. Средства отображения информации.

Практическая работа № 8

Тема: Выбор и обоснование средств подсистемы задержки

Цель: формирование подсистемы задержки нарушителя безопасности.

Формируемые компетенции: ПК 3.1, ПК 3.2, ПК 3.5, ОК 01 – 06, ОК 09, ОК 10

Задание 1.

Определение количества и типа рубежей физической защиты. В практической работе № 2 была определена категория объекта и сформулированы основные требования по технической укрепленности объекта защиты. В соответствии с этими требованиями должно быть определено количество рубежей защиты и класс защиты средств технической укрепленности объекта. Привести сведения о категории объекта и соответствующих ей классах защиты средств задержки в таблице:

Наименование средства задержки	Класс защиты
Количество рубежей защиты	
Основное ограждение	
Ворота, калитки	
Наличие шлагбаума	
Оконные конструкции	
Дверные конструкции	
Запорные устройства	
Наличие КПП	
Сейфы	
Шкафы	

Задание 2.

Выбор и обоснование основного ограждения. Провести выбор и обоснование основного ограждения. Привести характеристики основного ограждения в таблице:

Наименование	Характеристика
Высота ограждения	

Просматриваемость ограждения	
Деформируемость ограждения	
Вид полотна ограждения	
Материал опор ограждения	
Материал фундамента ограждения	
Тип установки ограждения	
Вид ограждения	

Задание 3.

Выбор и обоснование ворот и дверных конструкций. Провести выбор и обоснование ворот и дверных конструкций. Привести характеристики в таблице:

Наименование	Характеристика
Материал дверей	
Прочность	
Пулестойкость	
Способ открытия (наружу или внутрь)	
Толщина дверей	

Задание 4.

Выбор и обоснование запорных устройств. Провести выбор и обоснование запорных устройств. Привести характеристики в таблице:

Наименование	Характеристика
Вид замка на воротах	
Взломоустойчивость	
Вид замка входной двери	
Вид замка внутренних дверей	

Задание 5.

Выбор и обоснование оконных конструкций. Провести выбор и обоснование оконных конструкций. Привести характеристики в таблице:

Наименование	Характеристика
Защитные решётки, Жалюзи	
Тип и толщина стекла	
Материал оконных рам	

Задание 6.

Провести выбор и обоснование шкафов для хранения секретных документов и сейфов для хранения ценных документов и денежных средств. Привести характеристики в таблице:

Наименование	Характеристика
Материал шкафа	
Толщина стенок шкафа	
Вид замка шкафа	
Материал сейфа	
Вес сейфа	
Вид замка сейфа	

Содержание отчета

1. Таблица классов защиты для установленных рубежей защиты.

2. Характеристики основного ограждения объекта защиты
3. Характеристики ворот и дверных конструкций
4. Характеристики запорных устройств
5. Характеристики шкафов и сейфов для хранения секретных/ценных документов и денежных средств

Контрольные вопросы:

1. Определение количества и типа рубежей физической защиты.
2. Выбор и обоснование основного ограждения.
3. Выбор и обоснование ворот и дверных конструкций.
4. Выбор и обоснование запорных устройств.
5. Выбор и обоснование оконных конструкций.
6. Выбор и обоснование шкафов и сейфов.

Практическая работа № 9

Тема: Разработка структурной схемы и спецификации оборудования
Цель: построение структурной схемы физической защиты объекта.
Формируемые компетенции: ПК 3.1, ПК 3.2, ПК 3.5, ОК 01 – 06, ОК 09, ОК 10

Задание 1.

Разработка структурной схемы системы защиты объекта. При проектировании новой системы следует решить, как наилучшим образом интегрировать людей, процедуры и технические средства для решения задач СФЗИ. Первичными функциями СФЗИ являются обнаружение нарушителя, его задержание, а также реагирование персонала службы безопасности. Важно отметить, что для эффективного задержания должно произойти обнаружение. Приоритетная цель системы – защитить критичные ресурсы от хищения или диверсии со стороны злонамеренного лица. Для того чтобы система эффективно выполняла эту задачу, должно иметь место оповещение о нападении (задержка), что позволит самим силам реагирования прервать или остановить действия нарушителя.

Функции *СФЗ*

1. Обнаружение: использование извещателей охранной сигнализации; видеокамеры с детекторами движения.
2. Задержка: турникеты и ограждения на проходной; таблички с информацией о ведущемся видеонаблюдении.
3. Реагирование: использование системы оповещения; автоматическое реагирование системы; вызов уполномоченных органов защиты.

Пример структурной схемы физической защиты:

Задание 2.

Составить полную спецификацию оборудования физической защиты объекта. Пример спецификации оборудования приведен в таблице:

Наименование	Производитель	Количество	Примечание
СПД 3.3	НПФ «Полисервис»	61	Пожарный извещатель оптический комбинированный тепло-дымовой
КХ-08	OPTEX CO LTD	10	Извещатель охранный объемный потолочного крепления. Датчик движения, пассивный
Астра-642	НТЦ «ТЕКО»	22	Извещатель ультразвуковой, объемный, дальность 10 м, невосприимчивость к тепловым помехам. Датчик разбития стекла
Сигнал-20П (SMD)	«Болид»	1	Прибор приемно-контрольный охранно-пожарный на 20 шлейфов
ST-CE010EM	«Smartec»	2	Считыватель настольный для ввода идентификаторов EM. Контроль доступа к серверу
ST-SC141EHK	«Smartec»	5	Автономный вандалозащищенный контроллер со встроенными считывателем EM+HID
ML-194 K	«AccordTec»	6	Электромагнитный замок усилие не менее 500 кг с платой управления
MDC-AH7290FTD-24S	«MicroDigital Inc»	4	Купольная AHD камера для помещений, 2.0 Megapixel

Содержание отчета

1. Структурная схема системы защиты объекта
2. Спецификация оборудования физической защиты объекта

Контрольные вопросы:

1. Инженерно-технические средства физической защиты.
2. Методика проектирования системы физической защиты информации.
3. Структурная схема физической защиты.

Практическая работа № 10

Тема: Эксплуатация инженерно-технических средств физической защиты

Цель: изучить правила эксплуатации инженерно-технических средств физической защиты.

Формируемые компетенции: ПК 3.1, ПК 3.2, ПК 3.5, ОК 01 – 06, ОК 09, ОК 10

Задание 1.

Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта периметровых технических средств обнаружения.

Задание 2.

Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы контроля и управления доступом.

Задание 3.

Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы видеонаблюдения.

Задание 4.

Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы пожарной сигнализации.

Задание 5.

Опишите порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы охранной сигнализации.

Содержание отчета

Доклад с презентацией.

Тематика докладов:

1. Порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта периметровых технических средств обнаружения
2. Порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы контроля и управления доступом
3. Порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы видеонаблюдения
4. Порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы пожарной сигнализации
5. Порядок проведения технического обслуживания, установки, настройки, диагностики, организации ремонта системы охранной сигнализации

Контрольные вопросы:

1. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты.
2. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения.
3. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты.
4. Организация ремонта технических средств физической защиты.

СПИСОК ЛИТЕРАТУРЫ

Основная литература

1. Скрипник Д.А. Общие вопросы технической защиты информации: курс лекций / Скрипник Д.А. — Москва: Интуит НОУ, 2016. — 424 с. — URL: https://book.ru/book/917804 (дата обращения: 23.04.2021). — Текст: электронный.
2. Москвитин Г.И. Комплексная защита информации в организации: монография / Москвитин Г.И. — Москва: Русайнс, 2020. — 354 с. — ISBN 978-5-4365-1561-8. — URL: https://book.ru/book/934814 (дата обращения: 23.04.2021). — Текст: электронный.
3. Сагдеев К.М. Физические основы защиты информации Бакалавриат: учебное пособие / Сагдеев К.М., Петренко В.И., Чипига А.Ф. — Ставрополь: Северо-Кавказский федеральный университет, 2015. — 394 с. — URL: https://book.ru/book/928736 (дата обращения: 23.04.2021). — Текст: электронный.

Дополнительная литература

1. Гребенюк Е.И. Технические средства информатизации: учебник для студентов СПО / Е.И. Гребенюк, Н.А. Гребенюк. - М.: Издательский центр "Академия", 2014г.
2. Лавровская О.Б. Технические средства информатизации. Практикум: учебное пособие для студентов СПО. - М.: Издательский центр "Академия", 2013г.
3. Руденков Н.А. Технологии защиты информации в компьютерных сетях: курс лекций / Руденков Н.А., Пролетарский А.В., Смирнова Е.В., Суровов А.М. — Москва : Интуит НОУ, 2016. — 368 с. — URL: https://book.ru/book/918258 (дата обращения: 23.04.2021). — Текст: электронный
4. Тараскин М.М. Комплексная защита информации в организации: монография / Тараскин М.М., и др. — Москва: Русайнс, 2017. — 353 с. — ISBN 978-5-4365-1561-8. — URL: https://book.ru/book/922538 (дата обращения: 23.04.2021). — Текст: электронный
5. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
7. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий
8. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
9. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
10. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети
11. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
12. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

13. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
14. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности
15. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
16. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
17. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
18. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
19. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
20. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
21. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
22. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
23. Номенклатура показателей качества. Ростехрегулирование, 2005.
24. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
25. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
26. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
27. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
28. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
29. ГОСТ Р 50776-95 (МЭК 60839-1-4:1989) «Системы тревожной сигнализации»
30. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
31. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

32. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
33. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
34. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
35. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
36. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

Интернет ресурсы

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
9. Сайт Научной электронной библиотеки www.elibrary.ru