ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»

Комплект контрольно-оценочных средств

по

МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

для специальности

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Алексеевка – 2021

Комплект контрольно-оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 года № 1553.

Составитель:
Зюбан Е.В., преподаватель ОГАПОУ «Алексеевский колледж»

СОДЕРЖАНИЕ

1. Паспорт комплекта оценочных средств

1.1 Область применения комплекта оценочных средств

В соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования (далее – ФГОС СПО) колледж самостоятельно планирует результаты обучения по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации, которые соотнесены с требуемыми результатами освоения образовательной программы (компетенциями выпускников). Совокупность запланированных результатов обучения должна обеспечивать выпускнику освоение всех общих компетенций (далее – ОК), профессиональных компетенций (далее – ПК), установленных ФГОС СПО.

Контрольно-оценочные средства (далее - КОС) предназначены для контроля и оценки образовательных достижений обучающихся по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации.

КОС включают типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, и (или) практического опыта, характеризующих этапы формирования компетенций в процессе освоения образовательной программы для проведения текущего контроля успеваемости обучающихся и организации промежуточной аттестации в форме экзамена.

КОС разработан на основании рабочей программы МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации.

1.2 Планируемые результаты освоения междисциплинарного курса:

В результате освоения междисциплинарного курса обучающийся должен **уметь**:

У1. применять технические средства для криптографической защиты информации конфиденциального характера;

У2. применять технические средства для уничтожения информации и носителей информации;

У3. применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;

У4. применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;

У5. применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

У6. применять инженерно-технические средства физической защиты объектов информатизации.

В результате освоения междисциплинарного курса обучающийся должен **знать**:

З1. порядок технического обслуживания технических средств защиты информации;

З2. номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;

З3. 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;

З4. порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

З5. методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

З6. номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

З7. основные принципы действия и характеристики технических средств физической защиты;

З8. основные способы физической защиты объектов информатизации;

З9. номенклатуру применяемых средств физической защиты объектов информатизации.

В результате освоения междисциплинарного курса обучающийся должен **иметь практический опыт:**

ПО1. установки, монтажа и настройки технических средств защиты информации;

ПО2. технического обслуживания технических средств защиты информации;

ПО3. применения основных типов технических средств защиты информации;

ПО4. выявления технических каналов утечки информации;

ПО5. участия в мониторинге эффективности технических средств защиты информации;

ПО6. диагностики, устранения отказов и неисправностей, восстановления работоспособности технических средств защиты информации;

ПО7. проведения измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов

информатизации, для которой установлен режим конфиденциальности, при аттестации объектов информатизации по требованиям безопасности информации;

ПО8. проведения измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;

ПО9. установки, монтажа и настройки, технического обслуживания, диагностики, устранения отказов и неисправностей, восстановления работоспособности инженерно-технических средств физической защиты.

Профессиональные и общие компетенции, которые формируются при изучении междисциплинарного курса:

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 традиционных 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 языках.

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.

Планируемые личностные результаты освоения рабочей программы междисциплинарного курса:

ЛР 4. Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»

ЛР 7. Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.

ЛР 9. Соблюдающий и пропагандирующий правила здорового и безопасного образа жизни, спорта; предупреждающий либо преодолевающий зависимости от алкоголя, табака, психоактивных веществ, азартных игр и т.д. Сохраняющий психологическую устойчивость в ситуативно сложных или стремительно меняющихся ситуациях.

ЛР 10. Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой.

ЛР 11. Проявляющий уважение к эстетическим ценностям, обладающий основами эстетической культуры.

1.3 Контроль и оценка результатов освоения междисциплинарного курса

Таблица 1

Результаты (освоенные профессиональные компетенции) с учетом личностных результатов, профессионального стандарта и стандарта компетенции Ворлдскиллс	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического бслуживания технических средств защиты информации в	тестирование, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса. Экзамен

соответствии с требованиями эксплуатационной документации	соответствии с требованиями эксплуатационной документации	
ПК 3.2 Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации	Проявлять умения и практического опыта в эксплуатации технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса. Экзамен
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	Проводить работы по измерению параметров побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа	тестирование, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса. Экзамен
ПК 3.4 Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	Проводить самостоятельные измерения параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации	тестирование, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса. Экзамен
ПК 3.5 Организовывать отдельные работы по физической защите объектов информатизации	Проявлять знания в выборе способов решения задач по организации отдельных работ по физической защите объектов информатизации	тестирование, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса. Экзамен

2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, характеризующих этапы формирования компетенций в процессе освоения междисциплинарного курса для проведения текущего контроля успеваемости обучающихся

2.1. Тестовые задания

Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты

Задание № 1. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, З 1, З 2, З 3, У 1, У 2, У 3, У 6, ОК 1, ОК 2, ОК 10, ПК. 3.1, ПК.3.2)

Прочитайте текст и установите соответствие. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Запишите выбранные цифры под соответствующими буквами.

Соотнесите понятия с их определениями.

Понятие	**Определение**
a) Техническая защита	1) Совокупность методов и средств, направленных на предотвращение утечек информации
b) Инженерно-техническая защита	2) Подход, учитывающий взаимодействие всех элементов системы для достижения общей цели
c) Системный подход	3) Защита информации с помощью физических барьеров и технических устройств
d) Конфиденциальность	4) Свойство информации, заключающееся в недоступности для посторонних лиц

Запишите ответ:

a	
b	
c	
d	

Задание № 2 Прочитайте текст и установите последовательность. Ответ запишите в таблицу.

(оцениваемые практический опыт, знания, умения, компетенции: ПО 3, ПО 4, ПО 5, З 4, З 5, У 4, У 5, ОК 3, ОК 4, ПК. 3.3, ПК.3.4)

Расположите этапы разработки системы защиты информации в правильной последовательности.

1. Анализ требований и рисков
2. Выбор технических средств
3. Проектирование системы
4. Внедрение и тестирование
5. Оценка эффективности

Запишите ответ:

1	
2	

3	
4	
5	

Задание № 3 Задание на развернутый ответ

(оцениваемые практический опыт, знания, умения, компетенции ПО 6, ПО 7, ПО 8, ПО 9, З 6, З 7, У 5, У 6, ОК 1, ОК 5, ОК 6, ОК 7, ПК.3.1, ПК.3.5)

Прочитайте вопрос и ответ запишите.

Вопрос: _____- лицо, пытающееся проникнуть или проникшее в помещение (на территорию), защищенное системой охранной или охраннопожарной сигнализации без разрешения ответственного лица, пользователя, владельца, а также лицо, оказывающее ему содействие в этом.

Запишите ответ:_____

Задание № 4 Задание на выбор одного ответа

(оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 6, ПО 9, З 1, З 2, З 8, З 9, У 3, У 4, У 6, ОК 4, ОК 10, ПК.3.5)

Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

Вопрос: Что является основным принципом системного подхода при решении задач инженерно-технической защиты информации?

a) Минимизация затрат на реализацию проекта.

b) Учет всех взаимосвязей между элементами системы для достижения общей цели.

c) Максимальное упрощение процесса внедрения системы.

d) Использование самых современных технологий.

Запишите ответ: _____

Задание № 5 Практическое задание

(оцениваемые практический опыт, знания, умения, компетенции: ПО 6, ПО 7, ПО 9, З 4, З 6, З 7, З 9, У 3, У 5, У 6, ОК 1, ОК 2, ОК 10, ПК. 3.3, ПК.3.4, ПК.3.5)

Задание: Разработайте схему защиты информации для небольшой компании, учитывая следующие требования:

1. Компания работает с конфиденциальными данными клиентов.
2. Необходимо обеспечить защиту от несанкционированного доступа.
3. Бюджет ограничен.

Запишите ответ: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____
_____
_____
_____

Задание № 6 Ситуационное задание

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, ПО 6, ПО 8, ПО 9, З 1, З 3, З 5, З 6, З 9, У 2, У 4, У 5, У 6, ОК 8, ОК 9, ОК 10, ПК. 3.1, ПК.3.4, ПК.3.5)

Прочитайте ситуационную задачу и ответ запишите в таблицу

Задание: Вы являетесь руководителем отдела информационной безопасности крупной компании. Ваша компания планирует внедрить новую систему защиты информации. Определите основные шаги, которые нужно предпринять для успешного выполнения этого проекта.

Запишите ответ:

1	
2	
3	
4	
5	
6	

Задание № 7. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, З 1, З 2, З 8, У 1, У 4, ОК 3, ОК 4, ПК.3.5)

Прочитайте текст и установите соответствие. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Запишите выбранные цифры под соответствующими буквами.

Соотнесите принципы системного анализа с их описаниями.

Принцип	**Описание**
a) Целостность	1) Рассмотрение проблемы как части более широкой системы
b) Иерархичность	2) Учёт взаимозависимостей между различными аспектами проблемы
c) Многокритериальность	3) Возможность декомпозиции сложной системы на более простые компоненты
d) Динамичность	4) Изменчивость во времени, необходимость учёта изменений и адаптации системы

Запишите ответ:

a	

b	
c	
d	

Задание № 8 Прочитайте текст и установите последовательность. Ответ запишите в таблицу.

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, З 5, З 9, У 4, У 5, ОК 3, ОК 5, ОК 6, ПК. 3.1, ПК.3.2,)

Расположите этапы системного анализа в правильном порядке.

1. Постановка задачи
2. Сбор и анализ данных
3. Разработка альтернативных решений
4. Выбор оптимального решения
5. Реализация и оценка результатов

Запишите ответ:

1	
2	
3	
4	
5	

Задание № 9 Практическое задание

(оцениваемые практический опыт, знания, умения, компетенции: ПО 6, ПО 7, ПО 8, З 1, З 4, З 7, У 1, У 3, У 4, ОК 1, ОК 5, ОК 6, ОК 7, ОК 10, ПК.3.2ПК.3.4)

Задание: Разработайте классификацию способов и средств защиты информации, указав не менее пяти категорий и приведя примеры для каждой категории.

Запишите ответ: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Задание № 10 Задание на выбор одного ответа

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, ПО 3, З 1, З 2, У 5, У 6, ОК 3, ОК 4, ПК.3.5)

Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

Вопрос: Какие задачи решает инженерно-техническая защита информации?

a) Повышение производительности труда.

b) Обеспечение конфиденциальности, целостности и доступности информации.

c) Улучшение эргономики рабочих мест.

d) Увеличение прибыли компании.

Ключи ответов

Номер задания	Ответ
1	a-1, b-3, c-2, d-4
2	1, 3, 2, 4, 5
3	Нарушитель
4	b
5	Для начала проведем анализ рисков и определим наиболее вероятные угрозы. Затем выберем технические средства, такие как: 1. Шифрование данных; 2. Контроль доступа к информационным ресурсам; 3. Антивирусное программное обеспечение. Проектируем систему таким образом, чтобы она была максимально эффективной при ограниченном бюджете. Например, можно использовать бесплатные или недорогие программы для шифрования и контроля доступа. После внедрения проводим тестирование системы и оцениваем ее эффективность.
6	1. Проведение анализа текущих потребностей и существующих угроз. 2. Формулировка целей и задач проекта. 3. Разработка плана реализации проекта, включая выбор технических средств и разработку политик безопасности. 4. Внедрение системы защиты информации. 5. Тестирование и оценка эффективности новой системы. 6. Постоянный мониторинг и обновление системы для поддержания высокого уровня защиты.
7	a-1, b-3, c-2, d-4
8	1, 2, 3, 4, 5
9	1. Физическая защита: -Охранные системы (видеонаблюдение, сигнализация). -Ограждения и замки. 2. Программно-аппаратная защита: -Межсетевые экраны (firewalls). -Антивирусные программы.

	3. Криптографическая защита: -Шифрование данных. -Электронная подпись. 4. Организационная защита: -Политика информационной безопасности. -Процедуры контроля доступа. 5. Правовая защита: -Законы и нормативные акты. -Договоры о неразглашении информации.
10	b

Критерии оценивания ответов, полученных в ходе тестирования

За каждый верный ответ выставляется 1 балл, за неверный ответ – 0 баллов. Баллы, полученные обучающимися за выполненные задания, суммируются.

Результаты тестирования определяются в разрезе каждого обучающегося в баллах и оценках.

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**
0-4 баллов	2 (неудовлетворительно)	0-40%	низкий
5-6 баллов	3 (удовлетворительно)	50-60%	базовый
7-8 баллов	4 (хорошо)	70-80%	повышенный
9-10 баллов	5 (отлично)	90%-100%	высокий

Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты

Задание № 1. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 9, З 8, З 9, У 4, У 5, ОК 4, ОК 5, ПК.3.5)

Прочитайте текст и установите соответствие. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Запишите выбранные цифры под соответствующими буквами.

Соотнесите методы и средства перехвата информации с их описанием:

№	**Методы и средства перехвата информации**	**Описание**
a	Электронные стетоскопы	1.Устройства для усиления слабых звуковых колебаний, передающихся через твердые поверхности
b	Технические средства акустической разведки	2.Получение информации путем прямого прослушивания разговоров без использования технических средств

c	Непосредственное подслушивание звуковой информации	3.Специальные приборы для перехвата и анализа акустических сигналов
d	Прослушивание информации направленными микрофонами	4.Использование микрофонов с узкой диаграммой направленности для захвата звука на расстоянии
e	Система защиты от утечки по акустическому каналу	5.Комплекс мер и устройств для предотвращения несанкционированного доступа к информации через звуки

Запишите ответ:

a	
b	
c	
d	
e	

Задание № 2 Прочитайте текст и установите последовательность. Ответ запишите в таблицу.

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, ПО 3, З 1, З 2, У 3, У 4, ОК 1, ОК 2, ПК. 3.1, ПК 3.5)

Расположите этапы установки системы защиты информации от утечки по проводному каналу в правильной последовательности:

а) установка экранирующих материалов на кабели и оборудование;
б) анализ существующих коммуникационных сетей и выявление уязвимых мест;
в) выбор подходящих технических средств для защиты;
г) оценка эффективности установленной системы защиты.

Запишите ответ:

1	
2	
3	
4	

Задание № 3 Задание на развернутый ответ

(оцениваемые практический опыт, знания, умения, компетенции: ПО 8, ПО 9, З 7, З 8, З 9, У 4, У 5, У 6, ОК 8, ОК 9, ОК 10, ПК. 3.1, ПК.3.4, ПК.3.5)

Прочитайте вопрос и запишите ответ

Вопрос: _____- охрана объекта от НСД основывается на существующей нормативно правовой базе, основу которой составляют ГОСТы и руководящие документы МВД России и т.п.; она должна реализовывать требования и положения существующего законодательства, стандартов и нормативно методических документов.

Запишите ответ:

Задание № 4 Задание на выбор одного ответа

(оцениваемые практический опыт, знания, умения, компетенции: ПО 5,

ПО 6, З 1, З 2, У 2, У 3, ОК 2, ОК 3, ПК.3.5)

Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

Какой метод применяется для перехвата звука на большом расстоянии?

a) Непосредственное подслушивание звуковой информации

b) Прослушивание информации направленными микрофонами

c) Электронные стетоскопы

d) Система защиты от утечки по акустическому каналу

Запишите ответ: _____

Задание № 5 Практическое задание

(оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 6, ПО 7, ПО 9, З 4, З 5, З 6, З 7, З 8, З 9, У 2, У 3, У 4, У 5, ОК 1, ОК 5, ОК 6, ОК 7, ПК. 3.1, ПК.3.2, ПК.3.5)

Задание: Проведите анализ уязвимостей помещения к утечке информации по акустическому каналу и предложите комплекс мер по защите.

Запишите ответ: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Задание № 6 Прочитайте ситуационную задачу, решите кейс и ответ запишите в таблицу

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, ПО 3, ПО 4, ПО 9, З 1, З 2, З 3, З 8, З 9, У 1, У 4, У 5, У 6, ОК 1, ОК 8, ОК 9, ОК 10, ПК.3.2, ПК.3.4, ПК.3.5, ПК 3.1)

Вы являетесь специалистом по защите информации в банке. Вам поручено разработать общий подход по организации защиты банкоматов от физического воздействия злоумышленников. Какие этапы общего подхода защиты информации Вы можете предложить?

Запишите ответ:

1.	
2.	

3.	
4.	
5.	

Задание № 7. В задании установите соответствие. Ответ запишите в таблицу.

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, З 5, З 6, З 7, У 1, У 4, У 6, ОК 1, ОК 6, ОК 10, ПК. 3.2, ПК.3.5)

Прочитайте текст и установите соответствие. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Запишите выбранные цифры под соответствующими буквами.

Соотнесите методы и средства перехвата информации с их описанием:

№	**Методы и средства перехвата информации**	**Описание**
a	Принцип работы микрофона и телефона	1. Меры и устройства для предотвращения несанкционированной аудиозаписи
b	Использование коммуникаций в качестве соединительных проводов	2.Передача данных через существующие коммуникационные сети
c	Негласная запись информации на диктофоны	3.Скрытая аудиозапись разговоров или других звуков
d	Системы защиты от диктофонов	4. Преобразование звуковых волн в электрические сигналы и обратно

Запишите ответ:

a	
b	
c	
d	

Задание № 8 Прочитайте текст и установите последовательность. Ответ запишите в таблицу.

(оцениваемые практический опыт, знания, умения, компетенции ПО 8, ПО 9, З 1, З 23 6У 1, У 2, У 5, ОК 1, ОК 2, ОК 6, ПК. 3.3, ПК.3.4,)

Расположите этапы установки системы защиты информации от утечки по проводному каналу в правильной последовательности:

a) Установка экранирующих материалов на кабели и оборудование.
b) Анализ существующих коммуникационных сетей и выявление уязвимых мест.
c) Выбор подходящих технических средств для защиты.
d) Оценка эффективности установленной **системы защиты.**

Запишите ответ:

1	

2	
3	
4	

Задание № 9 Прочитайте определение и запишите понятие. Недостающее слово запишите в строку ответа.

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, ПО 3, ПО 9, З 1, З 2, З 8, З 9, У 1, У 2, ОК 4, ОК 5, ОК 6, ПК.3.2)

Электронное устройство, включающее в свой состав датчик, схему обработки сигналов и схему принятия решения – это …….
Запишите ответ: _____

Задание № 10 Задание на выбор одного ответа
(оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 6, ПО 7, З 4, З 5, З 7, З 8, З 9, У 1, У 6, ОК 1, ОК 2, ОК 10, ПК.3.2)
Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.
Что из перечисленного является примером негласной записи информации?
a) Запись разговора на диктофон с согласия участников
b) Запись телефонного разговора с помощью специализированного ПО
c) Скрытая установка микрофона в офисе
d) Использование защищенного канала связи для передачи данных
Запишите ответ: _____
Задание № 11 Практическое задание
(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, З 1, З 2, У 1, У 2, У 3, ОК 5, ОК 6, ОК 7, ПК. 3.3, ПК.3.4)

Задание: Проведите анализ уязвимостей офисного помещения к утечке информации по проводному каналу и предложите комплекс мер по защите.
Запишите ответ: _____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 12 Ситуационное задание
(оцениваемые практический опыт, знания, умения, компетенции: ПО 6,

ПО 7, ПО 8, ПО 9, З 5, З 6, З 7, У 1, У 2, У 5, У 6, ОК 1, ОК 2, ОК 7, ОК 8, ОК 9, ОК 10, ПК.3.2, ПК. 3.3, ПК.3.5)

Прочитайте ситуационную задачу и ответ запишите в таблицу

Задание: Вы являетесь специалистом по информационной безопасности в крупной компании. Руководство обратилось к вам с просьбой оценить риски утечки конфиденциальной информации через проводной канал в одном из офисов. Опишите, какие шаги вы предпримете для решения этой задачи.

Запишите ответ:

1	
2	
3	
4	
5	

Задание № 13. Установите соответствие. Ответ запишите в таблицу.

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, ПО 7, ПО 8, З 3, З 4, З 9, У 1, У 5, У 6, ОК 1, ОК 2, ОК 8, ОК 9 ПК. 3.2, ПК.3.4)

Прочитайте текст и установите соответствие. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Запишите выбранные цифры под соответствующими буквами.

Соотнесите средства защиты с их назначением:

Средства защиты	**Назначение**
1. Электронные стетоскопы	а) предотвращение утечки информации через вибрации;
2. Лазерные системы подслушивания	б) перехват информации через вибрации поверхностей;
3. Гидроакустические преобразователи	в) перехват сигналов через водную среду;
4. Системы защиты информации от утечки по вибрационному каналу	г) усиление слабых звуковых колебаний.

Запишите ответ:

1.	
2.	
3.	
4.	

Задание № 14 Прочитайте текст и установите последовательность. Ответ запишите в таблицу.
(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, З 4, З 5, З 6, У 1, У 2, ОК 1, ОК 5, ОК 6, ПК. 3.1, ПК.3.5)

Расположите этапы установки системы защиты информации от утечки по вибрационному каналу в правильной последовательности:
а) Установка виброизолирующих материалов на стены и окна помещения.
б) Анализ потенциальных источников вибрационных сигналов (окна, двери, трубы).
в) Выбор подходящих технических средств для защиты.
г) Оценка эффективности установленной системы защиты.
Запишите ответ:

1.	
2.	
3.	
4.	

Задание № 15 Прочитайте утверждение и запишите пропущенное слово в строку ответа.

(оцениваемые практический опыт, знания, умения, компетенции ПО 4, ПО 5, ПО 6, ПО 7, ПО 8, ПО 93 3, З 4, З 5, З 6, З 7, У 1, У 2, У 4, У 6, ОК 3, ОК 4, ОК 5, ОК 6, ОК 9, ОК 10 ПК.3.2, ПК. 3.3, ПК.3.5)

……. - это устройство, преобразующее физические величины и характеристики (излучение, свет, звук, давление и т.п.) в электрический сигнал.
Запишите ответ:
_____

Задание № 16 Задание на выбор одного ответа
(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 6, З 1, З 6, З 7, У 1, У 2, У 3, ОК 1, ОК 9, ОК 10, ПК.3.5)
Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.
Какое средство используется для перехвата информации через водную среду?

a) Электронный стетоскоп
b) Лазерная система подслушивания
c) Гидроакустический преобразователь
d) Система защиты информации от утечки по вибрационному каналу
Запишите ответ:
_____

Задание № 17 Практическое задание
(оцениваемые практический опыт, знания, умения, компетенции: ПО 7, ПО 8, ПО 9, З 6, З 7, З 8, З 9, У 6, ОК 7, ОК 8, ОК 9, ОК 10, ПК. 3.1, ПК.3.2, ПК.3.5)

Задание: Проведите анализ уязвимостей помещения к утечке информации по вибрационному каналу и предложите комплекс мер по защите.
Запишите ответ: _____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 18 Ситуационное задание
(оцениваемые практический опыт, знания, умения, компетенцииПО 6, ПО 7, ПО 8, ПО 9, З 1, З 2, З 3, З 4, У 1, У 2У 6, ОК 1, ОК 6, ОК 7, ОК 10, ПК.3.2, ПК. 3.3, ПК.3.4)
Прочитайте ситуационную задачу и ответ запишите в таблицу
Задание: Вы являетесь специалистом по информационной безопасности в крупной компании. Руководство обратилось к вам с просьбой оценить риски утечки конфиденциальной информации через вибрационный канал в одном из помещений офиса. Опишите, какие шаги вы предпримете для решения этой задачи.
Запишите ответ:

1	
2	
3	
4	
5	

Задание № 19 Задание на выбор одного ответа
(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, З 5, З 6, З 7 У 3, У 4, У 5, ОК 4, ОК 5, ПК.3.5)

Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.
Что из перечисленного является средством защиты от утечки информации по электромагнитному каналу?
a) Экранирующий материал
b) Радиозакладка
c) Детектор радиопередач
d) Приемник информации с радиозакладок
Запишите ответ: _____

Задание № 20 Задание на выбор одного ответа. Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

(оцениваемые практический опыт, знания, умения, компетенции: ПО 6, ПО 7, З 4, З 5, У 3, У 4, ОК 1, ОК 2, ПК. 3.1.)

Какой из перечисленных методов относится к средствам защиты от утечки информации по электромагнитному каналу?
а) Прослушивание информации от радиотелефонов.
б) Прослушивание информации от работающей аппаратуры.
в) Прослушивание информации от радиозакладок.
г) Приемники информации с радиозакладок.
д) Прослушивание информации о пассивных закладках.
е) Системы защиты от утечки по электромагнитному каналу.

Запишите ответ: _____
Задание № 21 Задание на выбор одного ответа
(оцениваемые практический опыт, знания, умения, компетенции: ПО 3, ПО 4, З 4, З 5, У 4, У 5ОК 1, ОК 5, ОК 6, ПК.3.2,)
Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.
Что из перечисленного относится к номенклатуре средств защиты информации от несанкционированной утечки по электросетевому каналу?

a) Низкочастотное устройство съема информации
b) Высокочастотное устройство съема информации
c) Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу
Запишите ответ: _____
Задание № 22 Задание на выбор одного ответа
(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, ПО 9, З 4, З 9, У 1, У 2 ОК 3, ОК 9, ОК 10, ПК. 3.3,)
Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

Какие из перечисленных ниже средств относятся к системам защиты от утечки информации по электросетевому каналу?

a) Фильтры высоких частот
b) Экранированные кабели
c) Шифраторы данных
d) Активные системы подавления сигналов
Запишите ответ: _____
Задание № 23 Задание на выбор одного ответа
(оцениваемые практический опыт, знания, умения, компетенции: ПО 7, ПО 9, З 23 9, У 1, У 4, ОК 2, ОК 3, ПК.3.4,)
Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.
Какой из следующих элементов является частью телевизионной системы наблюдения?

a) Датчики движения
b) Камера видеонаблюдения
c) Сетевой коммутатор
d) Аудиорегистратор
Запишите ответ: _____
Задание № 24 Задание на выбор одного ответа. Выберите правильный ответ и обведите кружочком номер правильного ответа. Правильный ответ может быть только один.

(оцениваемые практический опыт, знания, умения, компетенции: ПО 7, ПО 8, , З 8, У 4, У 5, , ОК 7, ОК 10, ПК. 3.1, ПК.3.5)
Какой из перечисленных приборов относится к приборам ночного видения?
Предложенные варианты:

а) бинокль;
б) тепловизор;
в) фотоаппарат;
г) прицел дневного видения.

Задание № 25 Прочитайте утверждение и запишите пропущенное слово в строку ответа.
(оцениваемые практический опыт, знания, умения, компетенции ПО 6, ПО 7, ПО 8, ПО 9, З 6, З 7, У 5, У 6, ОК 1, ОК 5, ОК 6, ОК 7, ПК.3.4, ПК.3.5)

……. представляют собой однородные микропроцессорные устройства, выполненные на однотипной элементной базе.

Запишите ответ:

_____

Ключи ответов

Номер задания	Ответ
1	a-1, b-3, c-2, d-4, e-5
2	б, в, а, г
3	Законность
4	b) Прослушивание информации направленными микрофонами
5	**Решение:** 1. **Анализ уязвимостей:** ○ Провести осмотр всех стен, потолков, полов и окон в помещении. ○ Определить наличие и расположение потенциальных источников звука (люди, техника, коммуникации). ○ Измерить уровни фонового шума и определить возможные пути распространения звука. 2. **Меры по защите:** ○ Установить звукоизолирующие материалы на все потенциально уязвимые поверхности (например, специальные покрытия на стены, окна и двери). ○ Использовать активные системы подавления звука, такие как генераторы белого шума. ○ Ограничить доступ к помещению посторонним лицам и установить контроль за использованием аудиооборудования. ○ Регулярно проводить мониторинг состояния защитных систем и их эффективности.
6	1. Оценка текущего состояния. 2. Разработка плана мероприятий. 3. Реализация защитных мер. 4. Мониторинг и поддержка. 5. Документирование.
7	a-4, b-2, c-3, d-1
8	b →c → a → d
9	Детектор
10	c) Скрытая установка микрофона в офисе
11	1. **Анализ уязвимостей:** ○ Провести осмотр всех кабельных соединений и сетевого

	оборудования в помещении. ○ Определить наличие и расположение потенциальных точек подключения сторонних устройств. ○ Измерить уровни электромагнитных излучений и определить возможные пути утечки информации. 2. **Меры по защите:** ○ Установить экранирующие материалы на все кабельные соединения и сетевое оборудование. ○ Использовать системы шифрования данных при передаче по проводным каналам. ○ Ограничить доступ к кабельным трассам и оборудованию посторонним лицам. ○ Регулярно проводить мониторинг состояния защитных систем и их эффективности.
12	**План действий:** 1. **Оценка текущего состояния:** ○ Проведение аудита офисного помещения на предмет наличия потенциальных путей утечки информации через проводной канал (анализ кабельной инфраструктуры, сетевого оборудования, точек подключения). ○ Измерение уровней электромагнитных излучений и определение зон повышенной чувствительности к сигналам. 2. **Разработка плана мероприятий:** ○ Определение необходимых средств защиты (экранирование, шифрование, контроль доступа). ○ Составление сметы расходов на закупку и установку оборудования. 3. **Реализация защитных мер:** ○ Установка выбранных средств защиты в соответствии с планом. ○ Тестирование эффективности установленных систем. 4. **Мониторинг и поддержка:** ○ Организация регулярного мониторинга состояния защитных систем. ○ Проведение периодических проверок и обновлений оборудования при необходимости. 5. **Документирование:** ○ Оформление отчета о проведенных работах и рекомендациях по дальнейшим действиям. ○ Предоставление руководству компании полного пакета документов, подтверждающих выполнение задач по защите информации от утечки по проводному каналу.
13	1-г, 2-б, 3-в, 4-г

14	б, в, а, г
15	датчик
16	**с) Гидроакустический преобразователь**
17	1. **Анализ уязвимостей:** ○ Провести осмотр всех твердых поверхностей в помещении (стены, пол, потолок, окна, двери). ○ Определить наличие трубопроводов, вентиляционных каналов и других инженерных коммуникаций, способных передавать вибрации. ○ Измерить уровень фоновых шумов и вибраций в помещении. 2. **Меры по защите:** ○ Установить виброизолирующие материалы на все потенциально уязвимые поверхности (например, специальные покрытия на стены, окна и двери). ○ Использовать звукоизоляционные панели для снижения уровня передачи вибраций через стены и перегородки. ○ Применять активные системы подавления вибраций, такие как генераторы белого шума или специальные вибродемпфирующие устройства. ○ Регулярно проводить мониторинг состояния защитных систем и их эффективность.
18	**План действий:** 1. **Оценка текущего состояния:** ○ Проведение аудита помещения на предмет наличия потенциальных путей утечки информации через вибрационный канал (анализ строительных конструкций, инженерных коммуникаций, окон, дверей и т.д.). ○ Измерение уровней фонового шума и вибраций внутри и снаружи помещения. 2. **Разработка плана мероприятий:** ○ Определение необходимых средств защиты (виброизоляция, звукоизоляция, активные системы подавления вибраций). ○ Составление сметы расходов на закупку и установку оборудования. 3. **Реализация защитных мер:** ○ Установка выбранных средств защиты в соответствии с планом. ○ Тестирование эффективности установленных систем. 4. **Мониторинг и поддержка:** ○ Организация регулярного мониторинга состояния защитных систем. ○ Проведение периодических проверок и обновлений оборудования при необходимости. 5. **Документирование:**

	○ Оформление отчета о проведенных работах и рекомендациях по дальнейшим действиям. ○ Предоставление руководству компании полного пакета документов, подтверждающих выполнение задач по защите информации от утечки по вибрационному каналу.
19	a) Экранирующий материал
20	e
21	c) Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.
22	a) Фильтры высоких частот
23	b) Камера видеонаблюдения.
24	б
25	Контроллеры

Критерии оценивания ответов, полученных в ходе тестирования

За каждый верный ответ выставляется 1 балл, за неверный ответ – 0 баллов. Баллы, полученные обучающимися за выполненные задания, суммируются.

Результаты тестирования определяются в разрезе каждого обучающегося в баллах и оценках.

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**
0-12 баллов	2 (неудовлетворительно)	0-48%	низкий
13-16 баллов	3 (удовлетворительно)	52-64%	базовый
17-21 баллов	4 (хорошо)	68-82%	повышенный
22-25 баллов	5 (отлично)	86-100%	высокий

Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты

Задание № 1. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, З 1, З 2, З 3, У 1, У 2, У 3, У 6, ОК 1, ОК 2, ОК 10, ПК. 3.1, ПК.3.2)

Прочитайте текст и установите соответствие. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Запишите выбранные цифры под соответствующими буквами.

Соотнесите понятия с их определениями.

Понятие	**Определение**
a) Техническая защита	1) Совокупность методов и средств, направленных на предотвращение утечек информации
b) Инженерно-техническая	2) Подход, учитывающий взаимодействие всех элементов

защита	системы для достижения общей цели
c) Системный подход	3) Защита информации с помощью физических барьеров и технических устройств
d) Конфиденциальность	4) Свойство информации, заключающееся в недоступности для посторонних лиц

Запишите ответ:

a	
b	
c	
d	

Задание № 2 Прочитайте текст и установите последовательность. Ответ запишите в таблицу.

(оцениваемые практический опыт, знания, умения, компетенции: ПО 3, ПО 4, ПО 5, З 4, З 5, У 4, У 5, ОК 3, ОК 4, ПК. 3.3, ПК.3.4)

Расположите этапы разработки системы защиты информации в правильной последовательности.

6. Анализ требований и рисков
7. Выбор технических средств
8. Проектирование системы
9. Внедрение и тестирование
10. Оценка эффективности

Запишите ответ:

1	
2	
3	
4	
5	

Задание № 3. Прочитайте определение и запишите понятие. Недостающее слово запишите в строку ответа.

(оцениваемые практический опыт, знания, умения, компетенции ПО 6, ПО 7, ПО 8, ПО 9, З 6, З 7, У 5, У 6, ОК 1, ОК 5, ОК 6, ОК 7, ПК.3.4, ПК.3.5)

Процесс сравнения тех или иных идентификационных признаков, принадлежащих конкретному физическому лицу или объекту, с информацией, заложенной в памяти системы – это …..

Запишите ответ:

_____

Задание № 4 Задание на выбор одного ответа

(оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 6, ПО 9, З 1, З 2, З 8, З 9, У 3, У 4, У 6, ОК 4, ОК 10, ПК.3.5)

Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

Вопрос: Что является основным принципом системного подхода при решении задач инженерно-технической защиты информации?
a) Минимизация затрат на реализацию проекта.
b) Учет всех взаимосвязей между элементами системы для достижения общей цели.
c) Максимальное упрощение процесса внедрения системы.
d) Использование самых современных технологий.
Запишите ответ: _____
Задание № 5 Прочитайте ситуационное задание, решите кейс и ответ запишите в таблицу.
(оцениваемые практический опыт, знания, умения, компетенции: ПО 6, ПО 7, ПО 9, З 4, З 6, З 7, З 9, У 3, У 5, У 6, ОК 1, ОК 2, ОК 10, ПК. 3.1, ПК.3.4, ПК.3.5)

Вас пригласили на работу в небольшую компанию в должности техника по защите информации. Первое задание, которое Вы получили от руководителя – предложить 3 меры по защите информации, учитывая следующие требования:

- Компания работает с конфиденциальными данными клиентов.
- Необходимо обеспечить защиту от несанкционированного доступа.
- Бюджет ограничен.

Продумайте 3 меры по защите информации и запишите ответ ниже:

1.	
2.	
3.	

Задание № 6 Ситуационное задание
(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, ПО 6, ПО 8, ПО 9, З 1, З 3, З 5, З 6, З 9, У 2, У 4, У 5, У 6, ОК 8, ОК 9, ОК 10, ПК. 3.1, ПК.3.4, ПК.3.5)
Прочитайте ситуационную задачу и ответ запишите в таблицу
Задание: Вы являетесь руководителем отдела информационной безопасности крупной компании. Ваша компания планирует внедрить новую систему защиты информации. Определите основные шаги, которые нужно предпринять для успешного выполнения этого проекта.
Запишите ответ:

1	
2	
3	
4	
5	
6	

Задание № 7. В задании установите соответствие. Ответ запишите в таблицу. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, З 1, З 2, З 8, У 1, У 4, ОК 3, ОК 4, ПК.3.2)***

Прочитайте текст и установите соответствие. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Запишите выбранные цифры под соответствующими буквами.

Соотнесите элементы ИТЗИ с их описанием:

№	Элементы ИТЗИ	Описание
а)	Физическая защита объектов	1.Системы видеонаблюдения, датчики движения, сигнализация.
б)	Системы контроля управления доступом	2.Использование генераторов помех, активных фильтров для подавления нежелательных сигналов.
в)	Средства активной защиты	3.Механические и электронные системы ограничения физического проникновения в помещения.
г)	Технические средства обнаружения угроз	4.Средства мониторинга сетевой активности, анализаторы трафика.

Запишите ответ:

а)	
б)	
в)	
г)	

Задание № 8 Прочитайте текст и установите последовательность. Ответ запишите в таблицу.

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, З 5, З 9, У 4, У 5, ОК 3, ОК 5, ОК 6, ПК. 3.1, ПК.3.2,)

Расположите этапы системного анализа в правильном порядке.

1. Постановка задачи
2. Сбор и анализ данных
3. Разработка альтернативных решений
4. Выбор оптимального решения
5. Реализация и оценка результатов

Запишите ответ:

1	
2	
3	
4	
5	

Задание № 9 Практическое задание

(оцениваемые практический опыт, знания, умения, компетенции: ПО 6, ПО 7, ПО 8, З 1, З 4, З 7, У 1, У 3, У 4, ОК 1, ОК 5, ОК 6, ОК 7, ОК 10,

ПК.3.2ПК.3.4)

Задание: Разработайте классификацию способов и средств защиты информации, указав не менее пяти категорий и приведя примеры для каждой категории.
Запишите ответ: _____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 10 Задание на выбор одного ответа
(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, ПО 3, З 1, З 2, У 5, У 6, ОК 3, ОК 4, ПК.3.5)
Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.
Вопрос: Какие задачи решает инженерно-техническая защита информации?
a) Повышение производительности труда.
b) Обеспечение конфиденциальности, целостности и доступности информации.
c) Улучшение эргономики рабочих мест.
d) Увеличение прибыли компании.

Ключи ответов

Номер задания	Ответ
1	a-1, b-3, c-2, d-4
2	1, 3, 2, 4, 5
3	Идентификация
4	b
5	1. Шифрование данных. 2. Контроль доступа к информационным ресурсам. 3. Антивирусное программное обеспечение.
6	1. Проведение анализа текущих потребностей и существующих угроз. 2. Формулировка целей и задач проекта.

	3. Разработка плана реализации проекта, включая выбор технических средств и разработку политик безопасности. 4. Внедрение системы защиты информации. 5. Тестирование и оценка эффективности новой системы. 6. Постоянный мониторинг и обновление системы для поддержания высокого уровня защиты.
7	а-3, б-1, в-2, г-4
8	1, 2, 3, 4, 5
9	1. Физическая защита: -Охранные системы (видеонаблюдение, сигнализация). -Ограждения и замки. 2. Программно-аппаратная защита: -Межсетевые экраны (firewalls). -Антивирусные программы. 3. Криптографическая защита: -Шифрование данных. -Электронная подпись. 4. Организационная защита: -Политика информационной безопасности. -Процедуры контроля доступа. 5. Правовая защита: -Законы и нормативные акты. -Договоры о неразглашении информации.
10	b

Критерии оценивания ответов, полученных в ходе тестирования

За каждый верный ответ выставляется 1 балл, за неверный ответ – 0 баллов. Баллы, полученные обучающимися за выполненные задания, суммируются.

Результаты тестирования определяются в разрезе каждого обучающегося в баллах и оценках.

Результаты тестирования			
Баллы	**Оценка**	**Доля выполненных заданий**	**Уровень сформированности компетенций**
0-4 баллов	2 (неудовлетворительно)	0-40%	низкий
5-6 баллов	3 (удовлетворительно)	50-60%	базовый
7-8 баллов	4 (хорошо)	70-80%	повышенный
9-10 баллов	5 (отлично)	90%-100%	высокий

2.2. Вопросы для устного опроса.

Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты

Тема 1.1. Цели и задачи физической защиты объектов информатизации

Вопросы:

1. Какие основные цели преследует физическая защита объектов информатизации? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 1, ОК 10, ПК.3.2)***
2. Почему важна физическая защита информационных ресурсов? ***(оцениваемые знания, умения, компетенции З 2, З 8, У 6, ОК 1, ПК.3.3)***
3. Какие угрозы информационной безопасности можно предотвратить с помощью физической защиты? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 2, ОК 2, ПК.3.5)***
4. Назовите основные задачи, решаемые средствами физической защиты. ***(оцениваемые знания, умения, компетенции З 1, З 4, У 1, ОК 9, ПК.3.1)***
5. Как связаны задачи физической защиты с общей стратегией информационной безопасности? ***(оцениваемые знания, умения, компетенции З 5, З 7, У 3, ОК 3, ПК.3.2)***
6. Какие факторы влияют на выбор средств физической защиты для конкретного объекта? ***(оцениваемые знания, умения, компетенции З 4, З 6, У 5, ОК 4, ПК.3.1)***
7. Приведите примеры целей и задач физической защиты для разных типов объектов (офис, дата-центр, производственное предприятие). ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 8, ПК.3.4)***
8. Как физическая защита способствует снижению риска утечки конфиденциальной информации? ***(оцениваемые знания, умения, компетенции З 3, З 9, У 4, ОК 5, ПК.3.5)***
9. Что включает в себя концепция комплексной физической защиты объекта? ***(оцениваемые знания, умения, компетенции З 4, З 8, У 3, ОК 6, ПК.3.5)***
10. Как изменяется роль физической защиты в условиях цифровизации бизнеса? ***(оцениваемые знания, умения, компетенции З 5, З 7, У 2, ОК 8, ПК.3.1)***

Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты

Вопросы:

1. Что такое комплекс ИТСФЗ и для каких целей он предназначен? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 1, ОК 7, ПК.3.5)***
2. Какие компоненты входят в состав комплекса ИТСФЗ? ***(оцениваемые знания, умения, компетенции З 2, З 8, У 6, ОК 3, ПК.3.4)***
3. Каким образом обеспечивается взаимодействие различных компонентов комплекса ИТСФЗ? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 5, ОК 2, ПК.3.5)***
4. Какие критерии используются для оценки эффективности комплексов ИТСФЗ? ***(оцениваемые знания, умения, компетенции З 3, З 8, У 4, ОК 5, ПК.3.3)***
5. Какие нормативные документы регулируют создание и эксплуатацию комплексов ИТСФЗ? ***(оцениваемые знания, умения, компетенции З 4, З 7, У 3, ОК 4, ПК.3.1)***
6. Какие современные технологии используются в комплексах ИТСФЗ? ***(оцениваемые знания, умения, компетенции З 5, З 6, У 2, ОК 7, ПК.3.2)***
7. Какие проблемы могут возникать при интеграции различных компонентов комплекса ИТСФЗ? ***(оцениваемые знания, умения, компетенции З 5, З 9, У 1, ОК 6, ПК.3.3)***
8. Какие факторы влияют на выбор конкретных средств физической защиты для включения в комплекс ИТСФЗ? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 3, ОК 8, ПК.3.5)***
9. Какие преимущества имеет интегрированный подход к созданию комплексов ИТСФЗ? ***(оцениваемые знания, умения, компетенции З 2, З 7, У 4, ОК 2, ПК.3.4)***
10. Какие перспективы развития комплексов ИТСФЗ вы видите в ближайшем будущем? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 6, ОК 9, ПК.3.3)***

Раздел 2. Основные компоненты комплекса инженерно-технических средств физической защиты

Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты

Вопросы:

1. Какие основные задачи решает система обнаружения в комплексе ИТСФЗ? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 2, ОК 10, ПК.3.1)***
2. Какие типы сенсоров и датчиков используются в системах обнаружения? ***(оцениваемые знания, умения, компетенции З 1, З 9, У***

1, ОК 1, ПК.3.5)

3. Каково различие между пассивными и активными датчиками в системах обнаружения? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 3, ОК 2, ПК.3.5)***
4. Какие факторы могут влиять на точность работы системы обнаружения? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 1, ПК.3.2)***
5. Как обеспечивается устойчивость системы обнаружения к ложным срабатываниям? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 6, ОК 9, ПК.3.5)***
6. Какие современные технологии применяются в системах обнаружения? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 1, ОК 1, ПК.3.4)***
7. Какие преимущества имеют системы обнаружения на основе видеоаналитики? ***(оцениваемые знания, умения, компетенции З 4, З 5, У 5, ОК 1, ПК.3.5)***
8. Какие проблемы могут возникать при установке и настройке систем обнаружения? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 1, ОК 3, ПК.3.5)***
9. Какие требования предъявляются к размещению датчиков и сенсоров в системе обнаружения? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 4, ОК 7, ПК.3.5)***
10. Какие возможности предоставляет интеграция системы обнаружения с другими компонентами комплекса ИТСФЗ? ***(оцениваемые знания, умения, компетенции З 7, З 8, У 3, ОК 8, ПК.3.3)***

Тема 2.2. Система контроля и управления доступом
Вопросы:

1. Что такое СКУД и для чего она предназначена? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 2, ОК 3, ПК.3.4)***
2. Какие основные элементы входят в состав СКУД? ***(оцениваемые знания, умения, компетенции З 1, З 5, У 4, ОК 1, ПК.3.5)***
3. Какие существуют методы идентификации пользователей в СКУД? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 1, ОК 10, ПК.3.5)***
4. Как СКУД интегрируется с другими системами безопасности? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 3, ОК 9, ПК.3.3)***

5. Какие уровни доступа обычно устанавливаются в СКУД? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 5, ОК 1, ПК.3.5)***
6. Какие меры предпринимаются для предотвращения несанкционированного доступа? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 6, ОК 2, ПК.3.2)***
7. Каковы основные требования к надежности и устойчивости СКУД? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 3, ПК.3.5)***
8. Какие преимущества и недостатки имеет централизованная и децентрализованная архитектура СКУД? ***(оцениваемые знания, умения, компетенции З 2, З 3, У 2, ОК 8, ПК.3.5)***
9. Какие нормативные документы регулируют установку и эксплуатацию СКУД? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 4, ОК 1, ПК.3.1)***
10. Какие современные технологии используются в СКУД? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 4, ОК 7, ПК.3.5)***
11. Какие данные собираются и хранятся в СКУД? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 1, ОК 6, ПК.3.1)***
12. Как СКУД обеспечивает безопасность персональных данных? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 5, ОК 5, ПК.3.5)***
13. Какие перспективы развития СКУД можно ожидать в ближайшие годы? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 5, ОК 4, ПК.3.3)***

Тема 2.3. Система телевизионного наблюдения

Вопросы:

1. Что такое система телевизионного наблюдения и для чего она используется? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 2, ОК 9, ПК.3.5)***
2. Какие основные компоненты входят в состав СТН? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 1, ОК 10, ПК.3.1)***
3. Какие типы камер используются в СТН? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 1, ПК.3.5)***
4. Как выбирается место установки камер в СТН? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 2, ОК 2, ПК.3.4)***
5. Какие методы записи и хранения видеоматериалов используются в СТН? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 1, ОК 4, ПК.3.5)***

6. Какие преимущества и недостатки имеет аналоговая и цифровая системы видеонаблюдения? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 3, ОК 3, ПК.3.5)***
7. Какие нормативные документы регулируют установку и эксплуатацию СТН? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 6, ОК 5, ПК.3.3)***
8. Какие меры предпринимаются для обеспечения безопасности данных в СТН? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 5, ОК 9, ПК.3.5)***
9. Какие современные технологии используются в СТН? ***(оцениваемые знания, умения, компетенции З 1, З 5, У 3, ОК 1, ПК.3.1)***
10. Какие требования предъявляются к освещенности при установке камер СТН? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 4, ОК 8, ПК.3.5)***
11. Какие перспективные направления развития СТН можно ожидать в ближайшие годы? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 6, ОК 7, ПК.3.5)***
12. Какие данные собираются и хранятся в СТН? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 1, ОК 6, ПК.3.2)***
13. Какие юридические аспекты следует учитывать при установке и эксплуатации СТН? ***(оцениваемые знания, умения, компетенции З 2, З 9, У 3, ОК 1, ПК.3.5)***

Тема 2.4. Система сбора, обработки, отображения и документирования информации

Вопросы:

1. Что представляет собой система сбора, обработки, отображения и документирования информации? ***(оцениваемые знания, умения, компетенции З 3, З 7, У 2, ОК 2, ПК.3.3)***
2. Какие основные компоненты входят в состав данной системы? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 1, ПК.3.5)***
3. Какие методы сбора данных используются в системе? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 10, ПК.3.5)***
4. Какие технологии обработки данных применяются в системе? ***(оцениваемые знания, умения, компетенции З 3, З 4, У 6, ОК 3, ПК.3.5)***
5. Какие форматы представления информации поддерживаются системой? ***(оцениваемые знания, умения, компетенции З 5, З 9, У 3, ОК 9,***

ПК.3.4)

6. Какие требования предъявляются к интерфейсу системы? ***(оцениваемые знания, умения, компетенции З 7, З 8, У 4, ОК 8, ПК.3.5)***
7. Какие меры предпринимаются для обеспечения безопасности данных в системе? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 4, ПК.3.1)***
8. Какие нормативные документы регулируют сбор, обработку и хранение данных? ***(оцениваемые знания, умения, компетенции З 3, З 4, У 1, ОК 5, ПК.3.5)***
9. Какие современные технологии используются в системах сбора, обработки и отображения информации? ***(оцениваемые знания, умения, компетенции З 5, З 6, У 1, ОК 5, ПК.3.2)***
10. Какие требования предъявляются к качеству собираемых данных? ***(оцениваемые знания, умения, компетенции З 7, З 9, У 5, ОК 7, ПК.3.5)***
11. Какие перспективные направления развития систем сбора, обработки и отображения информации можно ожидать в ближайшие годы? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 4, ОК 1, ПК.3.3)***
12. Какие данные собираются и хранятся в системе? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 2, ОК 6, ПК.3.5)***
13. Какие юридические аспекты следует учитывать при сборе, обработке и документировании информации? ***(оцениваемые знания, умения, компетенции З 1, З 5, У 3, ОК 4, ПК.3.1)***

Тема 2.5 Система воздействия

Вопросы:

1. Что такое телефонный канал утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 5, ОК 2, ПК.3.3)***
2. Какие основные источники утечки информации по телефонным линиям могут существовать? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 1, ПК.3.5)***
3. Какие методы используются для перехвата информации по телефонным каналам? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 1, ОК 10, ПК.3.5)***
4. Каковы основные компоненты систем защиты от утечки информации по телефонному каналу? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 6, ОК 5, ПК.3.4)***
5. Какие технические средства используются для защиты информации от

утечки по телефонным линиям? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 2, ОК 6, ПК.3.5)***

6. Как работает система шифрования телефонных разговоров? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 1, ПК.3.1)***
7. Какие меры принимаются для защиты телефонных линий от несанкционированного подключения? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 3, ОК 7, ПК.3.5)***
8. Как производится оценка эффективности систем защиты от утечки информации по телефонному каналу? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 2, ОК 9, ПК.3.2)***
9. Какие нормативные документы регламентируют установку и эксплуатацию систем защиты от утечки информации по телефонному каналу? ***(оцениваемые знания, умения, компетенции З 1, З 5, У 4, ОК 8, ПК.3.3)***
10. Каковы современные тенденции в развитии систем защиты от утечки информации по телефонному каналу? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 3, ОК 1, ПК.3.1)***
11. Какие сложности могут возникнуть при установке и настройке систем защиты от утечки информации по телефонному каналу? ***(оцениваемые знания, умения, компетенции З 3, З 9, У 6, ОК 4, ПК.3.2)***
12. Как выбрать подходящую систему защиты от утечки информации по телефонному каналу для конкретного объекта? ***(оцениваемые знания, умения, компетенции З 4, З 8, У 5, ОК 3, ПК.3.5)***
13. Как осуществляется техническое обслуживание и обновление систем защиты от утечки информации по телефонному каналу? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 1, ПК.3.3)***

Раздел 3. Применение и эксплуатация инженерно-технических средств физической защиты

Тема 3.1 Применение инженерно-технических средств физической защиты

Вопросы:

1. Какие основные цели преследуются при применении технических средств защиты информации? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 4, ОК 1, ПК.3.1)***
2. Какие классы технических средств защиты информации выделяют? ***(оцениваемые знания, умения, компетенции З 2, З 7, У 3, ОК 10, ПК.3.5)***

3. Какие факторы следует учитывать при выборе технических средств защиты информации для конкретной информационной системы? ***(оцениваемые знания, умения, компетенции З 3, З 8, У 5, ОК 9, ПК.3.2)***
4. Какие методы и подходы используются для оценки эффективности применяемых технических средств защиты информации? ***(оцениваемые знания, умения, компетенции З 4, З 7, У 6, ОК 21, ПК.3.5)***
5. Какие современные технологии используются в технических средствах защиты информации? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 7, ПК.3.3)***
6. Какие нормативные документы и стандарты регулируют применение технических средств защиты информации в Российской Федерации? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 1, ОК 3, ПК.3.1)***
7. Какие меры предосторожности следует соблюдать при внедрении новых технических средств защиты информации? ***(оцениваемые знания, умения, компетенции З 2, З 5, У 2, ОК 6, ПК.3.5)***
8. Каковы основные этапы внедрения технических средств защиты информации в организацию? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 3, ОК 5, ПК.3.3)***
9. Какие сложности могут возникнуть при эксплуатации технических средств защиты информации? ***(оцениваемые знания, умения, компетенции З 2, З 9, У 4, ОК 4, ПК.3.2)***
10. Как обеспечить совместимость различных технических средств защиты информации в рамках единой информационной системы? ***(оцениваемые знания, умения, компетенции З 3, З 8, У 1, ОК 3, ПК.3.4)***
11. Как организовать обучение персонала работе с техническими средствами защиты информации? ***(оцениваемые знания, умения, компетенции З 4, З 5, У 6, ОК 1, ПК.3.5)***
12. Как часто следует проводить проверку и обновление технических средств защиты информации? ***(оцениваемые знания, умения, компетенции З 6, З 9, У 5, ОК 2, ПК.3.1)***
13. Какие перспективы развития технических средств защиты информации вы видите в ближайшем будущем? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 1, ПК.3.5)***

Тема 3.2. Эксплуатация инженерно-технических средств физической защиты
Вопросы:

1. Что включает в себя процесс эксплуатации технических средств защиты

информации? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 5, ОК 1, ПК.3.5)***

2. Какие требования предъявляются к персоналу, осуществляющему эксплуатацию технических средств защиты информации? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 3, ОК 1, ПК.3.5)***
3. Какие процедуры входят в регулярное техническое обслуживание технических средств защиты информации? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 6, ОК 1, ПК.3.4)***
4. Как проводится мониторинг состояния технических средств защиты информации во время их эксплуатации? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 2, ОК 1, ПК.3.5)***
5. Какие меры принимаются для обеспечения непрерывной работы технических средств защиты информации? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 1, ОК 1, ПК.3.3)***
6. Какие документы оформляются при проведении эксплуатационных работ с техническими средствами защиты информации? ***(оцениваемые знания, умения, компетенции З 1, З 5, У 6, ОК 1, ПК.3.2)***
7. Как организуется учет и хранение технических средств защиты информации? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 2, ОК 1, ПК.3.5)***
8. Какие действия предпринимаются в случае неисправности технических средств защиты информации? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 1, ОК 1, ПК.3.1)***
9. Как организована процедура замены устаревших технических средств защиты информации на новые? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 3, ОК 1, ПК.3.2)***
10. Какие меры принимаются для обеспечения информационной безопасности при эксплуатации технических средств защиты информации? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 4, ОК 1, ПК.3.5)***
11. Какие отчеты составляются по результатам эксплуатации технических средств защиты информации? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 5, ОК 1, ПК.3.3)***
12. Какие факторы могут повлиять на эффективность эксплуатации технических средств защиты информации? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 6, ОК 1, ПК.3.5)***
13. Какие перспективные технологии могут улучшить процесс эксплуатации технических средств защиты информации в будущем? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 1, ОК 1,***

ПК.3.4)

Критерии оценивания ответов на вопросы

«5» «отлично» – студент показывает глубокое и полное овладение содержанием программного материала по междисциплинарному курсу, в совершенстве владеет понятийным аппаратом и демонстрирует умение применять теорию на практике, решать различные практические и профессиональные задачи, высказывать и обосновывать свои суждения в форме грамотного, логического ответа (устного или письменного), а также высокий уровень овладение общими и профессиональными компетенциями и демонстрирует готовность к профессиональной деятельности;

«4» «хорошо» – студент в полном объеме освоил программный материал по междисциплинарному курсу, владеет понятийным аппаратом, хорошо ориентируется в изучаемом материале, осознанно применяет знания для решения практических и профессиональных задач, грамотно излагает ответ, но содержание, форма ответа (устного или письменного) имеют отдельные неточности, демонстрирует средний уровень овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«3» «удовлетворительно» – студент обнаруживает знание и понимание основных положений программного материала по междисциплинарному курсу, но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических и профессиональных задач, не умеет доказательно обосновать свои суждения, но при этом демонстрирует низкий уровень овладения общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«2» «неудовлетворительно» – студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал по междисциплинарному курсу, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, характеризующих этапы формирования компетенций в процессе освоения междисциплинарного

курса для организации промежуточной аттестации в форме экзамена

Для проведения промежуточной аттестации в форме экзамена используются настоящие контрольно-оценочные средства для оформления экзаменационных билетов. Количество экзаменационных билетов должно превышать количество студентов на 3.

ПРИМЕР ОФОРМЛЕНИЯ БИЛЕТА

Департамент образования Белгородской области
Областное государственное автономное профессиональное образовательное учреждение
«Алексеевский колледж»

МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

семестр 6 курс 3

группа 831

Билет № **1**

1. Характеристики потенциально опасных объектов.
2. Разработать модель системы защиты информации в MS Visio для здания спортивного комплекса и обосновать своё решение.

Преподаватель: _____ Е.В. Зюбан
(подпись)

3.1. Перечень вопросов.

1. Характеристики потенциально опасных объектов. ***(оцениваемые знания, умения, компетенции: З 1, З 4, У 4, ОК 10, ПК. 3.1, ПК.3.2)***
2. Модель нарушителя и способы его проникновения. ***(оцениваемые знания, умения, компетенции: З 2, З 4, У 1, ОК 1, ПК. 3.1, ПК.3.3)***
3. Особенности задач охраны различных типов объектов. ***(оцениваемые знания, умения, компетенции: З 1, З 5, У 4, ОК 2, ПК. 3.1, ПК.3.4)***
4. Общие принципы обеспечения безопасности объектов. ***(оцениваемые знания, умения, компетенции: З 2, З 6, У 2, ОК 2, ПК. 3.1, ПК.3.5)***
5. Классификация и состав интегрированных систем охраны. ***(оцениваемые знания, умения, компетенции: З 3, З 7, У 3, ОК 10, ПК. 3.1, ПК.3.5)***
6. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника. ***(оцениваемые знания, умения, компетенции: З 1, З 4, У 5, ОК 7, ПК. 3.1, ПК.3.2)***
7. Информационные основы построения системы охранной сигнализации. ***(оцениваемые знания, умения, компетенции: З 4, З 8, У 6, ОК 9, ПК. 3.1, ПК.3.4)***
8. Построение систем обеспечения безопасности объекта. ***(оцениваемые знания, умения, компетенции: З 5, З 9, У 2, ОК 1, ПК. 3.4, ПК.3.5)***

9. Объектовые средства обнаружения: назначение, устройство, принцип действия. ***(оцениваемые знания, умения, компетенции: З 1, З 4, У 4, ОК 8, ПК. 3.1, ПК.3.2)***
10. Место системы контроля и управления доступом (СКУД) ***(оцениваемые знания, умения, компетенции: З 2, З 4, У 1, ОК 4, ПК. 3.1, ПК.3.3)***
11. Классификация средств управления доступом. ***(оцениваемые знания, умения, компетенции: З 3, З 4, У 5, ОК 5, ПК. 3.1, ПК.3.4)***
12. Методы удостоверения личности, применяемые в СКУД. ***(оцениваемые знания, умения, компетенции: З 1, З 5, У 5, ОК 6, ПК. 3.1, ПК.3.4)***
13. Обнаружение металлических предметов и радиоактивных веществ. ***(оцениваемые знания, умения, компетенции: З 1, З 6, У 5, ОК 3, ПК. 3.1, ПК.3.2)***
14. Аналоговые и цифровые системы видеонаблюдения. ***(оцениваемые знания, умения, компетенции: З 1, З 7, У 6, ОК 7, ПК. 3.1, ПК.3.2)***
15. Состав системы телевизионного наблюдения. ***(оцениваемые знания, умения, компетенции: З 1, З 7, У 6, ОК 8, ПК. 3.3, ПК.3.5)***
16. Инфракрасные осветители. Детекторы движения. ***(оцениваемые знания, умения, компетенции: З 1, З 8, У 4, ОК 2, ПК. 3.4, ПК.3.5)***
17. Классификация системы сбора и обработки информации.Негласная запись информации на диктофоны. ***(оцениваемые знания, умения, компетенции: З 1, З 9, У 1, ОК 9, ПК. 3.1, ПК.3.2)***
18. Варианты структур построения системы сбора и обработки информации. ***(оцениваемые знания, умения, компетенции: З 4, У 4, ОК 1, ПК. 3.3, ПК.3.4)***
19. Устройства отображения и документирования информации. ***(оцениваемые знания, умения, компетенции: З 3, З 4, У 1, ОК 10, ПК. 3.4, ПК.3.5)***
20. Назначение и классификация технических средств воздействия. ***(оцениваемые знания, умения, компетенции: З 5, З 9, У 1, ОК 1, ПК. 3.1, ПК.3.3)***
21. Периметровые и объектовые средства обнаружения, порядок применения. ***(оцениваемые знания, умения, компетенции: З 6, З 7, У 2, ОК 2, ПК. 3.1, ПК.3.4)***
22. Порядок применения устройств отображения и документирования информации. ***(оцениваемые знания, умения, компетенции: З 1, З 4, У 4, ОК 1, ПК. 3.1, ПК.3.5)***
23. Управление системой воздействия. ***(оцениваемые знания, умения, компетенции: З 2, З 5, У 3, ОК 3, ПК. 3.2, ПК.3.3)***
24. Этапы эксплуатации технических средств физической защиты.

(оцениваемые знания, умения, компетенции: З 3, З 5, У 6, ОК 5, ПК. 3.3, ПК.3.4)

25. Организация ремонта технических средств физической защиты. ***(оцениваемые знания, умения, компетенции: З 4, З 6, У 4, ОК 4, ПК. 3.4, ПК.3.5)***
26. Комплексный подход к обеспечению физической защиты объектов информатизации ***(оцениваемые знания, умения, компетенции: З 5, З 7, У 4, ОК 6, ПК. 3.1, ПК.3.2)***
27. Инновационные технологии в сфере ИТСФЗ ***(оцениваемые знания, умения, компетенции: З 1, З 8, У 6, ОК 7, ПК. 3.1, ПК.3.2)***
28. Роль персонала в обеспечении физической защиты объектов ***(оцениваемые знания, умения, компетенции: З 1, З 9, У 5, ОК 8, ПК. 3.3, ПК.3.4)***
29. Методы маскировки и скрытия информации: физическое и техническое сокрытие ***(оцениваемые знания, умения, компетенции: З 1, З 5, У 3, ОК 9, ПК. 3.1, ПК.3.3)***
30. Биометрические системы контроля доступа: достоинства и недостатки ***(оцениваемые знания, умения, компетенции: З 3, З 4, У 5, ОК 10, ПК. 3.1, ПК.3.5)***

3.2. Перечень практических заданий.

1. Разработать модель системы защиты информации в MS Visio для здания спортивного комплекса и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 3, ПО 4, ПО 9, З 5, З 6, У 3, ПК. 3.1, ПК.3.3)***
2. Разработать модель системы защиты информации в MS Visio для здания склада предприятия и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 4, ПО 5, ПО 9, З 1, З 4, У 4, ПК. 3.1, ПК.3.2)***
3. Разработать модель системы защиты информации для здания оптовой продуктовой базы и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 4, ПО 5, ПО 9, З 3, З 4, У 4, ПК. 3.1, ПК.3.2)***
4. Разработать модель системы защиты информации для здания магазина стройматериалов и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 2, ПО 5, ПО 9, З 2, З 5, У 1, ПК. 3.4, ПК.3.5)***
5. Разработать модель системы защиты информации для здания службы скорой помощи и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 5, ПО 9, З 1, З 4, У 2, ПК. 3.1, ПК.3.2)***

6. Разработать модель системы защиты информации для здания овощной базы и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 3, ПО 5, ПО 9, З 2, З 8, У 4, ПК. 3.1, ПК.3.5)***
7. Разработать модель системы защиты информации для здания ж/д вокзала и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 6, ПО 5, ПО 9, З 5, З 6, У 5, ПК. 3.2, ПК.3.4)***
8. Разработать модель системы защиты информации для здания спорткомплекса и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 9, ПО 7, ПО 9, З 8, З 9, У 4, ПК. 3.3, ПК.3.5)***
9. Разработать модель системы защиты информации для здания нотариальной конторы и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 9, ПО 8, ПО 9, З 7, З 9, У 6, ОК 2, ПК. 3.2, ПК.3.3)***
10. Разработать модель системы защиты информации для здания дома детского творчества и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 8, ПО 9, З 3, З 6, У 6, ОК 1, ПК. 3.1, ПК.3.4)***
11. Разработать модель системы защиты информации для здания дома культуры и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 3, ПО 4, ПО 9, З 5, З 6, У 3, ПК. 3.1, ПК.3.3)***
12. Разработать модель системы защиты информации для здания торгового центра и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 4, ПО 5, ПО 9, З 1, З 4, У 4, ПК. 3.1, ПК.3.2)***
13. Разработать модель системы защиты информации для здания склада бытовой химии и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 4, ПО 5, ПО 9, З 3, З 4, У 4, ПК. 3.1, ПК.3.2)***
14. Разработать модель системы защиты информации для здания склада промышленных товаров и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 2, ПО 5, ПО 9, З 2, З 5, У 1, ПК. 3.4, ПК.3.5)***
15. Разработать модель системы защиты информации для здания склада одежды и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 5, ПО 9, З 1, З 4, У 2, ПК. 3.1, ПК.3.2)***
16. Разработать модель системы защиты информации для здания автоцентра и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 3, ПО 5, ПО 9, З 2, З 8, У 4, ПК. 3.1, ПК.3.5)***

17. Разработать модель системы защиты информации для здания лизинговой компании и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 6, ПО 5, ПО 9, З 5, З 6, У 5, ПК. 3.2, ПК.3.4)***
18. Разработать модель системы защиты информации для здания магазина оргтехники и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 9, ПО 7, ПО 9, З 8, З 9, У 4, ПК. 3.3, ПК.3.5)***
19. Разработать модель системы защиты информации для здания кафе и обосновать своё решение.***(оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 9, ПО 8, ПО 9, З 7, З 9, У 6, ОК 2, ПК. 3.2, ПК.3.3)***
20. Разработать модель системы защиты информации для здания налоговой инспекции и обосновать своё решение. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 8, ПО 9, З 3, З 6, У 6, ОК 1, ПК. 3.1, ПК.3.4)***
21. Разработать модель системы защиты информации для здания фанерный комбинат и обосновать своё решение. (оцениваемые практический опыт, знания, умения, компетенции: ПО 4, ПО 5, ПО 9, З 3, З 4, У 4, ПК. 3.1, ПК.3.2)
22. Разработать модель системы защиты информации для здания адвокатской конторы и обосновать своё решение. (оцениваемые практический опыт, знания, умения, компетенции: ПО 2, ПО 5, ПО 9, З 2, З 5, У 1, ПК. 3.4, ПК.3.5)
23. Разработать модель системы защиты информации для здания заправочной станции и обосновать своё решение. (оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 5, ПО 9, З 1, З 4, У 2, ПК. 3.1, ПК.3.2)
24. Разработать модель системы защиты информации для здания музея и обосновать своё решение. (оцениваемые практический опыт, знания, умения, компетенции: ПО 3, ПО 5, ПО 9, З 2, З 8, У 4, ПК. 3.1, ПК.3.5)
25. Разработать модель системы защиты информации для здания администрации и обосновать своё решение. (оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 6, ПО 5, ПО 9, З 5, З 6, У 5, ПК. 3.2, ПК.3.4)
26. Разработать модель системы защиты информации для здания ресторана и обосновать своё решение. (оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 9, ПО 7, ПО 9, З 8, З 9, У 4, ПК. 3.3, ПК.3.5)
27. Разработать модель системы защиты информации для здания автомагазина и обосновать своё решение. (оцениваемые практический

опыт, знания, умения, компетенции: ПО 5, ПО 9, ПО 8, ПО 9, З 7, З 9, У 6, ОК 2, ПК. 3.2, ПК.3.3)

28. Разработать модель системы защиты информации для здания школы и обосновать своё решение. (оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 8, ПО 9, З 3, З 6, У 6, ОК 1, ПК. 3.1, ПК.3.4)

Критерии оценивания

«5» «отлично» – студент показывает глубокое и полное овладение содержанием программного материала по междисциплинарному курсу, в совершенстве владеет понятийным аппаратом и демонстрирует умение применять теорию на практике, решать различные практические и профессиональные задачи, высказывать и обосновывать свои суждения в форме грамотного, логического ответа (устного или письменного), а также высокий уровень овладение общими и профессиональными компетенциями и демонстрирует готовность к профессиональной деятельности;

«4» «хорошо» – студент в полном объеме освоил программный материал по междисциплинарному курсу, владеет понятийным аппаратом, хорошо ориентируется в изучаемом материале, осознанно применяет знания для решения практических и профессиональных задач, грамотно излагает ответ, но содержание, форма ответа (устного или письменного) имеют отдельные неточности, демонстрирует средний уровень овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«3» «удовлетворительно» – студент обнаруживает знание и понимание основных положений программного материала по междисциплинарному курсу, но излагает его неполно, непоследовательно, допускает неточности в определении понятий, в применении знаний для решения практических и профессиональных задач, не умеет доказательно обосновать свои суждения, но при этом демонстрирует низкий уровень овладения общими и профессиональными компетенциями и готовность к профессиональной деятельности;

«2» «неудовлетворительно» – студент имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определении понятий, беспорядочно и неуверенно излагает программный материал по междисциплинарному курсу, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует

овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

4. Информационное обеспечение

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Гребенюк Е. И., Гребенюк Н. А. Технические средства информатизации. Учебник для СПО М.: ИЦ Академия,2019 – 352 с.
2. Техническая защита информации в объектах информационной инфраструктуры (1-е изд.) учебник Бубнов А.А.,М.: ИЦ Академия, 2019 – 272 с.

Дополнительные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.
2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015
3. Новиков В.К. Организационное и правовое обеспечение информационнойбезопасности: В 2-х частях. Часть 2 Организационное обеспечение информационной безопасности: учеб.пособие. – М.: МИЭТ, 2013 – 172 с.
4. Организационно-правовое обеспечениеИнформационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов,В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017 – 336с
5. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие -Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.
6. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации Академия, - 336 с. – 2012
7. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд во: ДМК Пресс, - 2012
8. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012 – 416 с.

9. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
10. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
11. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
12. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
13. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
14. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
15. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
16. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
17. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
18. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
19. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
20. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
21. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
22. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и

производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.
23. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России
24. от 30 августа 2002 г. № 282.
25. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
26. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России
27. от 31 августа 2010 г. № 416/489.
28. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.
29. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.
30. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.
31. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».
32. 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
33. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий
34. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер
35. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

36. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью
37. 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
38. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности
39. 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
40. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"
41. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"
42. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
43. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.
44. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.
45. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.
46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
47. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
48. Номенклатура показателей качества. Ростехрегулирование, 2005.
49. 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.
50. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

51. 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.
52. 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.
53. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
54. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
55. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.
56. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
57. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
58. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. УтвержденГостехкомиссией России, 2002.
59. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
60. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
61. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Электронные издания (электронные ресурсы):

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с.

2. https://urait.ru/bcode/456793
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с.
4. https://urait.ru/bcode/449548
5. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с.
6. https://urait.ru/bcode/451933
7. Интерфейсы периферийных устройств – https://intuit.ru/studies/courses/92/92/lecture/28396
8. О компонентах системного блока — подробно – https://intuit.ru/studies/courses/3685/927/lecture/19564?page=2
9. Портативные компьютеры – https://intuit.ru/studies/courses/13910/1276/lecture/24146
10. Сравнительные характеристики процессоров – https://intuit.ru/studies/courses/15812/478/lecture/21074
11. Технические средства информационных технологий – https://intuit.ru/studies/courses/3481/723/lecture/14240
12. Устройства ввода информации – https://intuit.ru/studies/courses/3460/702/lecture/14158
13. Устройства вывода информации – https://intuit.ru/studies/courses/3460/702/lecture/14157
14. Цифровая образовательная среда СПО PROFобразование:
    - Старостин, А. А. Технические средства автоматизации и управления : учебное пособие для СПО / А. А. Старостин, А. В. Лаптева ; под редакцией Ю. Н. Чеснокова. — 2-е изд. — Саратов, Екатеринбург : Профобразование, Уральский федеральный университет, 2019. — 168 с. — ISBN 978-5-4488-0503-5, 978-5-7996-2842-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87882 (дата обращения: 31.08.2020). — Режим доступа: для авторизир. пользователей

Электронно-библиотечная система:
IPR BOOKS - http://www.iprbookshop.ru/78574.html

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moodle.alcollege.ru/