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

Комплект контрольно-оценочных средств

по

МДК.03.01 Техническая защита информации

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
1.2 Планируемые результаты освоения междисциплинарного курса
1.3. Контроль и оценка результатов освоения междисциплинарного курса
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
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
4. Информационное обеспечение

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.03.01 Техническая защита информации, 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.03.01 Техническая защита информации.

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.03.01 Техническая защита информации.

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 соответствии с требованиями эксплуатационной документации	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	тестирование, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса. Экзамен

ПК 3.2 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. Концепция инженерно-технической защиты информации

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.3.3)

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

Понятие	Определение
1. Техническая защита	а) совокупность методов и средств, направленных на предотвращение утечек информации;
2. Инженерно-техническая защита	б) подход, учитывающий взаимодействие всех элементов системы для достижения общей цели;
3. Системный подход	в) защита информации с помощью физических барьеров и технических устройств;
4. Конфиденциальность	г) свойство информации, заключающееся в недоступности для посторонних лиц.

Запишите ответ:

1.	
2.	
3.	
4.	

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.3.4, ПК.3.5)

Прочитайте вопрос и ответ запишите в таблицу.

Вопрос: Опишите, какие основные параметры следует учитывать при проектировании системы защиты информации.

Запишите ответ:

1	
2	
3	
4	
5	
6	

Задание № 4 Выберите правильный ответ и обведите кружочком номер правильного ответа. Правильный ответ может быть только один.

(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)

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

а) минимизация затрат на реализацию проекта;

б) учет всех взаимосвязей между элементами системы для достижения общей цели;

в) максимальное упрощение процесса внедрения системы;

г) использование самых современных технологий.

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**
1. Целостность	а) рассмотрение проблемы как части более широкой системы;
2. Иерархичность	б) учёт взаимозависимостей между различными аспектами проблемы;
3. Многокритериальность	в) возможность декомпозиции сложной системы на более простые

	компоненты;
4. Динамичность	г) изменчивость во времени, необходимость учёта изменений и адаптации системы.

Запишите ответ:

1.	
2.	
3.	
4.	

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. Предложенные варианты:

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 Выберите правильный вариант ответа и обведите кружочком номер правильного ответа. Правильный ответ может быть только один.

(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)

Вопрос: Какие задачи решает инженерно-техническая защита информации?

а) Повышение производительности труда.
б) Обеспечение конфиденциальности, целостности и доступности информации.
в) Улучшение эргономики рабочих мест.
г) Увеличение прибыли компании.

Ключи ответов

Номер задания	Ответ
1	1-а, 2-в, 3-б, 4-г
2	1, 3, 2, 4, 5
3	1. Степень критичности защищаемой информации; 2. Возможные угрозы и уязвимости; 3. Бюджет компании; 4. Соответствие нормативным требованиям; 5. Требования к доступности и надежности системы; 6. Совместимость с существующей инфраструктурой.
4	б
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	1-а, 2-в, 3-б, 4-г
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	б

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. Теоретические основы инженерно-технической защиты информации

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

(оцениваемые практический опыт, знания, умения, компетенции: ПО 3, ПО 4, З 8, З 9, У 3, У 6, ОК 4, ОК 9, ОК 10, 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 понятия с их определениями.

Термин	**Определение**
a) Техническая защита	2) Совокупность методов и средств, направленных на предотвращение утечки информации через технические каналы.
b) Шифрование	1) Процесс обработки данных с целью их преобразования в форму, недоступную для несанкционированного доступа.
c) Криптография	3) Наука о методах обеспечения конфиденциальности, целостности и аутентичности информации.

Запишите ответ:

a	
b	
c	

Задание № 2 В задании установите правильную последовательность.

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

Расположите следующие шаги в правильной последовательности для установки системы защиты информации:

а) выбор технических средств защиты;
б) оценка текущих рисков;
в) анализ требований к защите информации;
г) установка и настройка системы;
д) мониторинг и поддержка системы.

Запишите ответ:

1.	
2.	
3.	
4.	
5.	

Задание № 3 Задание на развернутый ответ

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 7, ПО 9, З 2, З 7, З 8, З 9, У 3, У 5, У 6, ОК 5, ОК 6, ОК 8, ОК 9, ПК. 3.3, ПК.3.4, ПК.3.5)

Прочитайте вопрос и ответ запишите в таблицу.

Вопрос: Опишите основные принципы инженерно-технической защиты

информации и приведите примеры их реализации.

Запишите ответ:

1	
2	
3	
4	
5	
6	

Задание № 4 Задание на выбор одного ответа
(оцениваемые практический опыт, знания, умения, компетенции: ПО 8, ПО 9, З 1, З 2, У 4, У 5, ОК 3, ОК 4, ПК.3.5)
Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

Вопрос: Какой из перечисленных ниже методов относится к физическим мерам защиты информации?

a) Использование антивирусного программного обеспечения
b) Контроль доступа к помещениям
c) Шифрование данных
d) Фильтрация трафика в сети
Запишите ответ: _____

Задание № 5 Практическое задание
(оцениваемые практический опыт, знания, умения, компетенции:, ПО 5, ПО 6, ПО 7, ПО 8, ПО 9, З 3, З 4, З 5, З 6, З 7, У 2, У 4, У 6, ОК 3, ОК 7, ОК 10, ПК.3.2, ПК. 3.3, ПК.3.5)

Задание: Составьте план мероприятий по защите информации в офисе компании, учитывая следующие аспекты:

- Защита от несанкционированного доступа к компьютерам
- Защита от утечки информации через акустические каналы
- Защита от перехвата данных в сети

Запишите ответ: _____
_____
_____
_____
_____
_____
_____
_____

_____
_____
_____
_____
_____

Задание № 6 Ситуационное задание

(оцениваемые практический опыт, знания, умения, компетенции: ПО 4, ПО 5, ПО 6, ПО 8, ПО 9, З 3, З 5, З 6, З 8, З 9, У 1, У 3, У 5, У 6, ОК 1, ОК 4, ОК 5, ПК. 3.3, ПК.3.4,)

Прочитайте ситуационную задачу и ответ запишите в таблицу

Задание: Представьте, что вы являетесь специалистом по защите информации в крупной компании. Ваша задача – разработать стратегию защиты корпоративной сети от внешних угроз. Опишите, какие меры вы предложите для защиты сети, включая технические и организационные аспекты.

Запишите ответ:

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

Задание № 7 Рассчитайте количество времени, необходимое для взлома пароля длиной 8 символов, если известно, что скорость перебора составляет 1000 комбинаций в секунду. Используйте предположение о том, что пароль состоит только из букв нижнего регистра латинского алфавита. ***(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 6, ПО 7, ПО 9, З 1, З 2, З 6, З 8, У 1, У 3, У 4, ОК 3, ОК 4ОК 7, ОК 9, ПК. 3.1, ПК.3.2, ПК.3.5)***

Прочитайте текст и решите задачу

Запишите ответ:

_____
_____
_____
_____
_____
_____
_____
_____
_____

_____
_____
_____
_____
_____
_____
_____

Ключи ответов

Номер задания	Ответ
1	a-2, b-1, c-3
2	в, б, а, г, д
3	Основные принципы инженерно-технической защиты информации включают: 1. Конфиденциальность: обеспечение того, чтобы доступ к информации имели только авторизованные пользователи. Пример: шифрование данных. 2. Целостность: гарантия того, что информация не была изменена без разрешения. Пример: использование цифровых подписей и хеш-функций. 3. Доступность: обеспечение доступности информации для авторизованных пользователей, когда это необходимо. Пример: резервное копирование и восстановление данных. 4. Аутентификация: проверка подлинности пользователя перед предоставлением ему доступа к информации. Пример: многофакторная аутентификация. 5. Журналирование и аудит: ведение записей всех операций с информацией для последующего анализа и расследования инцидентов. Пример: логирование событий безопасности.
4	b)
5	План: Защита от несанкционированного доступа к компьютерам: Установить сложные пароли на все рабочие станции. Использовать двухфакторную аутентификацию для входа в систему. Ограничить физический доступ к серверам и другим критически важным устройствам. Защита от утечки информации через акустические каналы: Провести звукоизоляцию помещений, где обсуждаются важные

	данные. Установить системы подавления акустических сигналов (шумогенераторы). Регулярно проверять помещения на наличие скрытых микрофонов. Защита от перехвата данных в сети: Использовать VPN для безопасного соединения сотрудников с корпоративной сетью. Применять шифрование трафика на уровне сетевых протоколов (TLS/SSL). Настроить межсетевые экраны для блокировки нежелательного трафика.
6	Стратегия: Технические меры: 1. Установка межсетевых экранов (firewalls) для фильтрации входящего и исходящего трафика. 2. Использование систем обнаружения вторжений (IDS/IPS) для раннего выявления подозрительной активности. 3. Внедрение регулярного сканирования уязвимостей и патч-менеджмента для своевременного устранения слабых мест. 4. Шифрование передаваемых данных внутри сети и при передаче через интернет. Организационные меры: 1. Обучение сотрудников основам кибербезопасности для предотвращения фишинга и других социальных инженерных атак. 2. Разработка политики паролей и управление привилегиями доступа для минимизации риска компрометации учетных записей. 3. Создание плана реагирования на инциденты для оперативного устранения последствий атак. 4. Постоянный мониторинг и аудит сетевой активности для быстрого обнаружения аномалий.
7	Решение: Количество возможных комбинаций для пароля длиной 8 символов, состоящего только из букв нижнего регистра (26 букв), равно 26^8. 26^8=208827064576 Теперь рассчитаем время, необходимое для перебора всех этих

	комбинаций со скоростью 1000 комбинаций в секунду: 208827064576/1000≈208827065 секунд Переводим секунды в более удобные единицы измерения: 208827065/60≈3480451 минут 3480451/60≈58008 часов 58008/24≈2417 дней 2417/365≈6.62 года Таким образом, потребуется примерно 6 лет и 8 месяцев для полного перебора всех возможных комбинаций пароля.

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**
0-3 баллов	2 (неудовлетворительно)	0-43%	низкий
4-5 баллов	3 (удовлетворительно)	57-72%	базовый
6 баллов	4 (хорошо)	72-86%	повышенный
7 баллов	5 (отлично)	87-100%	высокий

Раздел 3. Физические основы технической защиты информации

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, У 1, У 2, ОК 9, ОК 10, 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.

Установите соответствие между физическими методами защиты информации и их описаниями:

Метод защиты информации	**Описание**
а) Экранирование	1. Использование различных механизмов для ограничения доступа к объекту или информации.
б) Средства противодействия	2. Использование специальных экранов и покрытий для предотвращения утечек информации через

взлому	электромагнитные волны.
в) Контроль доступа	3. Использование укрепленных дверей, замков и других средств для затруднения несанкционированного доступа.

Запишите ответ:

а)	
б)	
в)	

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

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

Расположите следующие шаги в правильной последовательности для защиты информации в серверной комнате:

a) Установка систем кондиционирования воздуха

b) Монтаж систем видеонаблюдения

c) Ограничение физического доступа к помещению

d) Размещение серверов в стойках

Запишите ответ:

1	
2	
3	
4	
5	

Задание № 3 Задание на развернутый ответ

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

Прочитайте вопрос и ответ запишите

Вопрос: Объясните, как работает экранирование как метод защиты информации и приведите примеры его применения.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Задание № 4 Задание на выбор одного ответа

(оцениваемые практический опыт, знания, умения, компетенции: ПО 6, ПО 9, З 1, З 8, З 9, У 5, ОК 3, ОК 4, ОК 5, ОК 6, ПК. 3.3)

Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

Вопрос: Какой из перечисленных методов относится к физическим мерам защиты информации?

a) Шифрование данных
b) Блокировка USB-портов
c) Антивирусное ПО
d) Межсетевое экранирование

Запишите ответ: _____

Задание № 5 Практическое задание

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, ПО 5, ПО 9, З 3, З 5, З 8, З 9, У 1, У 5, У 6, ОК 1, ОК 4, ОК 5, ПК. 3.3, ПК.3.4, ПК.3.5)

Задание: Разработайте план защиты информации в офисе компании, учитывая следующие аспекты:

1. Защита от кражи данных через физические носители (USB-накопители)
2. Защита от несанкционированного доступа к рабочим станциям
3. Защита от физического повреждения оборудования

Запишите ответ: _____

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 6 Ситуационное задание

(оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 6, ПО 7, З 1, З 5, З 8, З 9, У 3, У 6, ОК 3, ОК 4, ОК 9, ОК 10, ПК. 3.1, ПК.3.2, ПК.3.5)

Прочитайте ситуационную задачу и ответ запишите в таблицу

Задание: Вы являетесь инженером по защите информации в банке. Вам поручено разработать меры по защите банкоматов от физического воздействия злоумышленников. Какие меры вы можете предложить?

Запишите ответ:

1	
2	
3	
4	
5	

Задание № 7. Прочитайте, решите задачу и запишите решение с ответом Определите, сколько времени потребуется злоумышленнику, чтобы получить доступ к данным на жестком диске, используя инструменты для снятия крышки корпуса компьютера и извлечения диска, если предполагается, что злоумышленник действует быстро и уверенно, но не обладает специальными навыками вскрытия сложных замков.
(оцениваемые практический опыт, знания, умения, компетенции: ПО 1ПО 3, ПО 4, ПО 6, З 6, З 9, У 5, У 6, ОК 6, ОК 7, ПК. 3.1, ПК.3.5)
Запишите ответ: _____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Ключи ответов

Номер задания	Ответ
1	а-2, б-3, в-1
2	d → a → c → b
3	Экранирование — это метод защиты информации, который предполагает создание барьера вокруг электронного устройства или кабеля для предотвращения утечки электромагнитных сигналов. Оно помогает защитить информацию от перехвата с помощью специальных материалов, блокирующих

	распространение электромагнитных волн. Экранирование может применяться различными способами: 1.Экран на кабелях: Специальные металлические оболочки или покрытия на кабелях помогают уменьшить электромагнитные излучения, предотвращая утечку информации. 2.Заземленные корпуса устройств: Использование металлических корпусов для компьютеров и другого оборудования позволяет эффективно гасить электромагнитные поля, снижая риск утечки информации. 3.Специальные комнаты: Для особо чувствительных данных могут использоваться специальные экранированные помещения («Faraday cage»), полностью изолированные от внешнего мира, чтобы исключить любые электромагнитные утечки. Примером экранирования может служить экранирующая комната, используемая для защиты особо важных данных в государственных учреждениях или крупных корпорациях.
4	b) Блокировка USB-портов
5	План: 1.Защита от кражи данных через физические носители: Отключить возможность использования USB-портов на рабочих станциях. Ввести политику запрета на использование личных накопителей сотрудниками. Установить программное обеспечение для отслеживания попыток подключения неизвестных устройств. 2.Защита от несанкционированного доступа к рабочим станциям: Ограничить доступ в офисное помещение с помощью пропускной системы. Использовать биометрическую идентификацию для доступа к оборудованию. Применить сложные пароли и двухфакторную аутентификацию для входа в операционные системы. 3.Защита от физического повреждения оборудования: Разместить оборудование в закрытых шкафах или стойках с замками. Установить камеры видеонаблюдения для мониторинга физического доступа к оборудованию. Проводить регулярные проверки оборудования на предмет повреждений и вмешательства.
6	Меры:

	1. Усиленная конструкция банкоматов: Использование прочных материалов для защиты от механических воздействий. 2. Установка датчиков движения и вибрации: Эти датчики могут обнаруживать попытки физического воздействия на банкоматы и сигнализировать об этом службе безопасности. 3. Использование систем видеонаблюдения: Камеры должны фиксировать все происходящее возле банкоматов для последующей идентификации нарушителей. 4. Ограниченный доступ к внутренним компонентам: Например, установка PIN-кодов для открытия сервисных панелей банкоматов. 5. Мониторинг окружающей среды: Слежение за температурой, влажностью и другими факторами, которые могут указывать на попытку вскрытия банкомата.
7	Предположим, что злоумышленнику требуется около 30 секунд, чтобы снять крышку корпуса компьютера и извлечь жесткий диск. Если у злоумышленника есть инструменты для вскрытия корпуса, то дополнительные навыки не требуются, так как большинство корпусов компьютеров легко открываются стандартными инструментами. Таким образом, злоумышленнику потребуется всего около 30 секунд для выполнения задачи.

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**
0-3 баллов	2 (неудовлетворительно)	0-43%	низкий
4-5 баллов	3 (удовлетворительно)	57-72%	базовый
6 баллов	4 (хорошо)	72-86%	повышенный
7 баллов	5 (отлично)	87-100%	высокий

Раздел 4. Системы защиты от утечки информации

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 3.2.)

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. 3.3, ПК.3.4, ПК.3.5)
Прочитайте вопрос и ответ запишите
Вопрос: Опишите основные принципы работы направленных микрофонов и их применение для перехвата информации.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

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.3.4, ПК.3.5)

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

Запишите ответ: _____
_____
_____
_____
_____

_____
_____
_____
_____
_____
_____
_____
_____

Задание № 6 Ситуационное задание

(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)

Прочитайте ситуационную задачу и ответ запишите в таблицу

Задание: Вы являетесь инженером по защите информации в банке. Вам поручено разработать меры по защите банкоматов от физического воздействия злоумышленников. Какие меры вы можете предложить?

Запишите ответ:

1	
2	
3	
4	
5	

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 5, З 6, З 7, У 1, У 4, У 6, ОК 1, ОК 6, ОК 10, ПК. 3.1, 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**
а)	Принцип работы микрофона и телефона	1. Меры и устройства для предотвращения несанкционированной аудиозаписи
б)	Использование коммуникаций	2.Передача данных через

	в качестве соединительных проводов	существующие коммуникационные сети
в)	Негласная запись информации на диктофоны	3.Скрытая аудиозапись разговоров или других звуков
г)	Системы защиты от диктофонов	4. Преобразование звуковых волн в электрические сигналы и обратно

Запишите ответ:

а)	
б)	
в)	
г)	

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. 3.2, ПК 3.1., ПК.3.4,)
Расположите следующие шаги в правильной последовательности для установки технических средств защиты информации:

а) Выбор технических средств защиты.
б) Оценка текущих рисков.
в) Анализ требований к защите информации.
г) Установка и настройка системы.
д) Мониторинг и поддержка системы.

Запишите ответ:

1.	
2.	
3.	
4.	
5.	

Задание № 9 Задание на развернутый ответ
(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.3.4,)
Прочитайте вопрос и ответ запишите
Вопрос: Опишите принцип работы микрофона и телефона и способы их применения для перехвата информации.

_____
_____
_____

_____
_____
_____
_____
_____
_____
_____
_____

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. В задании установите соответствие между понятием и его определением. 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. 3.3, 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
a	Электронные стетоскопы	1.Предотвращение утечки информации через вибрации
b	Лазерные системы подслушивания	2.Перехват информации через вибрации поверхностей
c	Гидроакустические преобразователи	3.Перехват сигналов через водную среду
d	Системы защиты информации от утечки по вибрационному каналу	4.Усиление слабых звуковых колебаний

Запишите ответ:

a	
b	
c	
d	

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:

a) Установка виброизолирующих материалов на стены и окна помещения.
b) Анализ потенциальных источников вибрационных сигналов (окна, двери, трубы).
c) Выбор подходящих технических средств для защиты.
d) Оценка эффективности установленной системы защиты.

Запишите ответ:

1	
2	
3	
4	

Задание № 15 Задание на развернутый ответ

(оцениваемые практический опыт, знания, умения, компетенцииПО 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 10ПК.3.2, ПК. 3.3, ПК.3.5)

Прочитайте вопрос и ответ запишите

Вопрос: Опишите основные принципы работы электронных стетоскопов и их применение для защиты информации от утечки по вибрационному каналу.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

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?
а) Экранирующий материал

b) Радиозакладка
c) Детектор радиопередач
d) Приемник информации с радиозакладок
Запишите ответ: _____

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

Какой из перечисленных методов относится к средствам защиты от утечки информации по электромагнитному каналу?

a) Прослушивание информации от радиотелефонов
b) Прослушивание информации от работающей аппаратуры
c) Прослушивание информации от радиозакладок
d) Приемники информации с радиозакладок
e) Прослушивание информации о пассивных закладках
f) Системы защиты от утечки по электромагнитному каналу
Запишите ответ: _____
Задание № 21 Выберите правильный ответ и обведите кружочком номер правильного ответа. Правильный ответ может быть только один.

(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,)

Что из перечисленного относится к номенклатуре средств защиты информации от несанкционированной утечки по электросетевому каналу?
а) Низкочастотное устройство съема информации.
б) Высокочастотное устройство съема информации.
в) 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
(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)
Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.
Какой из перечисленных приборов относится к приборам ночного видения?

a) Бинокль
b) Тепловизор
c) Фотоаппарат
d) Прицел дневного видения
Запишите ответ: _____
Задание № 25 Выберите правильный ответ и обведите кружочком номер правильного ответа. Правильный ответ может быть только один.
(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 6, З 5, З 6, У 1, У 2, ОК 1, ОК 2, , ПК.3.2)
Что из перечисленного относится к системам защиты информации по оптическому каналу? Предложенные варианты:

а) зеркальные стекла;
б) инфракрасные фильтры;
в) лазерные сканеры;
г) акустические экраны.

Ключи ответов

Номер задания	Ответ
1	a-1, b-3, c-2, d-4, e-5
2	б, в, а, г

3	Направленные микрофоны предназначены для улавливания звуков, исходящих из определенного направления, игнорируя шумы и звуки, приходящие с других направлений. Принцип их работы основан на использовании узкой диаграммы направленности, которая фокусирует прием звука только в пределах заданного угла. Это достигается за счет специальной конструкции микрофона, включающей несколько капсюлей или длинное тело, которое помогает отсекать нежелательные звуки. Применение направленных микрофонов особенно эффективно в ситуациях, когда необходимо перехватывать разговоры на значительном расстоянии или в условиях повышенного шума. Например, они могут использоваться для записи переговоров в открытых пространствах, таких как парки, площади или конференц-залы. Направленный микрофон можно направить на конкретный источник звука, чтобы минимизировать влияние посторонних шумов и улучшить качество записи. Однако стоит отметить, что использование направленных микрофонов требует определенных условий, таких как стабильная позиция источника звука и отсутствие сильных помех. Кроме того, современные системы защиты от утечек информации часто включают меры противодействия направленным микрофонам, например, генерацию маскирующего шума или использование активных систем подавления акустических сигналов.
4	b) Прослушивание информации направленными микрофонами
5	**Решение:** 1. **Анализ уязвимостей:** o Провести осмотр всех стен, потолков, полов и окон в помещении. o Определить наличие и расположение потенциальных источников звука (люди, техника, коммуникации). o Измерить уровни фонового шума и определить возможные пути распространения звука. 2. **Меры по защите:** o Установить звукоизолирующие материалы на все потенциально уязвимые поверхности (например, специальные покрытия на стены, окна и двери). o Использовать активные системы подавления звука, такие как генераторы белого шума. o Ограничить доступ к помещению посторонним лицам и установить контроль за использованием аудиооборудования. o Регулярно проводить мониторинг состояния защитных систем и их эффективности.

6	**План действий:** **Оценка текущего состояния:** 1. Проведение аудита помещения на предмет наличия потенциальных путей утечки информации через акустический канал (анализ строительных конструкций, расположения мебели, источников звука). 2. Измерение уровней фонового шума и определение зон повышенной чувствительности к звуковым сигналам. **Разработка плана мероприятий:** 1. Определение необходимых средств защиты (звукоизоляция, активные системы подавления звука, контроль доступа). 2. Составление сметы расходов на закупку и установку оборудования. **Реализация защитных мер:** 1. Установка выбранных средств защиты в соответствии с планом. 2. Тестирование эффективности установленных систем. **Мониторинг и поддержка:** 1. Организация регулярного мониторинга состояния защитных систем. 2. Проведение периодических проверок и обновлений оборудования при необходимости. **Документирование:** 1. Оформление отчета о проведенных работах и рекомендациях по дальнейшим действиям. 2. Предоставление руководству компании полного пакета документов, подтверждающих выполнение задач по защите информации от утечки по акустическому каналу.
7	а-4, б-2, в-3, г-1
8	в, б, а, г, д
9	Микрофон и телефон основаны на принципе преобразования звуковых волн в электрические сигналы и наоборот. Микрофон улавливает звуковые волны и преобразует их в электрический ток, который затем передается по проводу или радиосигналу. Телефон, в свою очередь, принимает этот электрический сигнал и преобразует его обратно в звуковые волны, позволяя слышать речь или другой звук. Для перехвата информации эти устройства могут быть использованы различными способами. Например, микрофон может быть скрытно установлен в помещении для негласной записи разговоров. Телефон также может быть использован для прослушивания, если злоумышленник получает доступ к линии связи или использует специальное оборудование для перехвата

	радиосигналов. Современные системы защиты от утечек информации включают в себя различные меры, направленные на предотвращение несанкционированного использования микрофонов и телефонов. К ним относятся экранирование кабелей и оборудования, шифрование передаваемых данных, а также использование специальных устройств для обнаружения и блокирования несанкционированных записей.
10	c) Скрытая установка микрофона в офисе
11	1. **Анализ уязвимостей:** o Провести осмотр всех кабельных соединений и сетевого оборудования в помещении. o Определить наличие и расположение потенциальных точек подключения сторонних устройств. o Измерить уровни электромагнитных излучений и определить возможные пути утечки информации. 2. **Меры по защите:** o Установить экранирующие материалы на все кабельные соединения и сетевое оборудование. o Использовать системы шифрования данных при передаче по проводным каналам. o Ограничить доступ к кабельным трассам и оборудованию посторонним лицам. o Регулярно проводить мониторинг состояния защитных систем и их эффективности.
12	**План действий:** 1. **Оценка текущего состояния:** o Проведение аудита офисного помещения на предмет наличия потенциальных путей утечки информации через проводной канал (анализ кабельной инфраструктуры, сетевого оборудования, точек подключения). o Измерение уровней электромагнитных излучений и определение зон повышенной чувствительности к сигналам. 2. **Разработка плана мероприятий:** o Определение необходимых средств защиты (экранирование, шифрование, контроль доступа). o Составление сметы расходов на закупку и установку оборудования. 3. **Реализация защитных мер:** o Установка выбранных средств защиты в соответствии с планом. o 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	a-4, b-2, c-3, d-1
14	b →c → a → d
15	Электронные стетоскопы представляют собой устройства, предназначенные для усиления слабых звуковых колебаний, которые могут передаваться через твердые поверхности, такие как стены, полы, потолки и другие строительные конструкции. Они работают путем преобразования механических вибраций в электрические сигналы, которые затем усиливаются и анализируются оператором. В контексте защиты информации электронные стетоскопы используются для обнаружения попыток несанкционированного прослушивания через вибрационные каналы. Оператор может использовать такой прибор для мониторинга возможных точек утечки информации, таких как окна, двери, водопроводные трубы и другие элементы здания, способные передавать вибрации. Это позволяет своевременно выявлять потенциальные угрозы и принимать меры по их устранению.
16	**c) 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	f) Системы защиты от утечки по электромагнитному каналу.
21	в
22	a) Фильтры высоких частот
23	b) Камера видеонаблюдения.
24	b) Тепловизор.
25	б

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 5. Применение и эксплуатация технических средств защиты информации

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 6, З 7, У 2, У 3, ОК 1, ОК 2, ПК. 3.1)

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.

Установите соответствие между техническими средствами защиты информации и их функциями:

Средства защиты	**Функция**
Антивирусное ПО	В. Защита от вредоносного ПО
Межсетевой экран	Б. Защита от несанкционированного доступа
VPN	Г. Создание защищенного канала связи
Системы контроля доступа	Д. Управление правами доступа

Запишите ответ:

a	
b	
c	

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

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

Расположите этапы установки межсетевого экрана в правильной последовательности:

1. Выбор подходящего устройства или программы
2. Установка программного обеспечения
3. Настройка правил фильтрации трафика
4. Тестирование работоспособности

Запишите ответ:

1	
2	
3	
4	
5	

Задание № 3 Задание на развернутый ответ

(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 5, ПО 6, З 3, З 4, З 5, У 5, У 6, ОК 3, ОК 7, ОК 8, ПК.3.4, ПК.3.5)

Прочитайте вопрос и ответ запишите

Вопрос: Объясните, как работает экранирование как метод защиты информации и приведите примеры его применения.

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 4 Задание на выбор одного ответа

(оцениваемые практический опыт, знания, умения, компетенции: ПО 7, З 8, У 1, ОК 1, ПК.3.5)

Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

Вопрос: Какой из перечисленных методов относится к физическим мерам защиты информации?

a) Шифрование данных
b) Блокировка USB-портов
c) Антивирусное ПО
d) Межсетевое экранирование

Задание № 5 Практическое задание

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

Задание: Разработайте план защиты информации в офисе компании, учитывая следующие аспекты:

4. Защита от кражи данных через физические носители (USB-накопители)
5. Защита от несанкционированного доступа к рабочим станциям
6. Защита от физического повреждения оборудования

Запишите ответ: _____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Задание № 6 Ситуационное задание
(оцениваемые практический опыт, знания, умения, компетенции ПО 4, ПО 5, ПО 6, ПО 9, З 1, З 4, З 7, У 2, У 4, У 6, ОК 4, ОК 10, ПК. 3.1, ПК. 3.3,)
Прочитайте ситуационную задачу и ответ запишите в таблицу
Задание: Вы являетесь инженером по защите информации в банке. Вам поручено разработать меры по защите банкоматов от физического воздействия злоумышленников. Какие меры вы можете предложить?
Запишите ответ:

1	
2	
3	
4	
5	

Задание № 7. Прочитайте, решите задачу и запишите решение с ответом
Определите, сколько времени потребуется злоумышленнику, чтобы получить доступ к данным на жестком диске, используя инструменты для снятия крышки корпуса компьютера и извлечения диска, если предполагается, что злоумышленник действует быстро и уверенно, но не обладает специальными навыками вскрытия сложных замков.
(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, ПО 9, З 4, З 5, З 9, У 1, У 3, У 5, ОК 3, ОК 6, ОК 8, ПК.3.2, ПК.3.5)
Запишите ответ: _____
_____
_____
_____
_____

_____
_____
_____
_____
_____
_____
_____
_____

Ключи ответов

Номер задания	Ответ
1	Антивирусное ПО — В. Защита от вредоносного ПО Межсетевой экран — Б. Защита от несанкционированного доступа VPN — Г. Создание защищенного канала связи Системы контроля доступа — Д. Управление правами доступа
2	1 → 2 → 3 → 4
3	Экранирование — это метод защиты информации, который предполагает создание барьера вокруг электронного устройства или кабеля для предотвращения утечки электромагнитных сигналов. Оно помогает защитить информацию от перехвата с помощью специальных материалов, блокирующих распространение электромагнитных волн. Экранирование может применяться различными способами: 1.Экран на кабелях: Специальные металлические оболочки или покрытия на кабелях помогают уменьшить электромагнитные излучения, предотвращая утечку информации. 2.Заземленные корпуса устройств: Использование металлических корпусов для компьютеров и другого оборудования позволяет эффективно гасить электромагнитные поля, снижая риск утечки информации. 3.Специальные комнаты: Для особо чувствительных данных могут использоваться специальные экранированные помещения («Faraday cage»), полностью изолированные от внешнего мира, чтобы исключить любые электромагнитные утечки. Примером экранирования может служить экранирующая комната, используемая для защиты особо важных данных в государственных учреждениях или крупных корпорациях.
4	b) Блокировка USB-портов

5	План: 1.Защита от кражи данных через физические носители: Отключить возможность использования USB-портов на рабочих станциях. Ввести политику запрета на использование личных накопителей сотрудниками. Установить программное обеспечение для отслеживания попыток подключения неизвестных устройств. 2.Защита от несанкционированного доступа к рабочим станциям: Ограничить доступ в офисное помещение с помощью пропускной системы. Использовать биометрическую идентификацию для доступа к оборудованию. Применить сложные пароли и двухфакторную аутентификацию для входа в операционные системы. 3.Защита от физического повреждения оборудования: Разместить оборудование в закрытых шкафах или стойках с замками. Установить камеры видеонаблюдения для мониторинга физического доступа к оборудованию. Проводить регулярные проверки оборудования на предмет повреждений и вмешательства.
6	Меры: 6. Усиленная конструкция банкоматов: Использование прочных материалов для защиты от механических воздействий. 7. Установка датчиков движения и вибрации: Эти датчики могут обнаруживать попытки физического воздействия на банкоматы и сигнализировать об этом службе безопасности. 8. Использование систем видеонаблюдения: Камеры должны фиксировать все происходящее возле банкоматов для последующей идентификации нарушителей. 9. Ограниченный доступ к внутренним компонентам: Например, установка PIN-кодов для открытия сервисных панелей банкоматов. 10. Мониторинг окружающей среды: Слежение за температурой, влажностью и другими факторами, которые могут указывать на попытку вскрытия банкомата.
7	Предположим, что злоумышленнику требуется около 30 секунд, чтобы снять крышку корпуса компьютера и извлечь жесткий

	диск. Если у злоумышленника есть инструменты для вскрытия корпуса, то дополнительные навыки не требуются, так как большинство корпусов компьютеров легко открываются стандартными инструментами. Таким образом, злоумышленнику потребуется всего около 30 секунд для выполнения задачи.

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**
0-3 баллов	2 (неудовлетворительно)	0-43%	низкий
4-5 баллов	3 (удовлетворительно)	57-72%	базовый
6 баллов	4 (хорошо)	72-86%	повышенный
7 баллов	5 (отлично)	87-100%	высокий

2.2. Вопросы для устного опроса.

Раздел 1. Концепция инженерно-технической защиты информации

Тема 1.1. Предмет и задачи технической защиты информации

Вопросы:

1. Что такое техническая защита информации (ТЗИ)? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 1, ОК 10, ПК.3.2)***
2. Какие основные цели преследует ТЗИ? ***(оцениваемые знания, умения, компетенции З 2, З 8, У 6, ОК 1, ПК.3.3)***
3. В чем заключается отличие между ТЗИ и информационной безопасностью? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 2, ОК 2, ПК.3.5)***
4. Какие виды угроз для информации существуют? Приведите примеры. ***(оцениваемые знания, умения, компетенции З 1, З 4, У 1, ОК 9, ПК.3.1)***
5. Каковы основные принципы организации системы ТЗИ? ***(оцениваемые знания, умения, компетенции З 5, З 7, У 3, ОК 3, ПК.3.2)***
6. Какие методы и средства используются для обеспечения ТЗИ? ***(оцениваемые знания, умения, компетенции З 4, З 6, У 5, ОК 4,***

ПК.3.1)

7. Какие нормативные документы регулируют деятельность в области ТЗИ в Российской Федерации? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 8, ПК.3.4)***
8. Что включает в себя комплекс мероприятий по защите информации от утечки по техническим каналам? ***(оцениваемые знания, умения, компетенции З 3, З 9, У 4, ОК 5, ПК.3.5)***
9. Какие технические каналы утечки информации вы знаете? ***(оцениваемые знания, умения, компетенции З 4, З 8, У 3, ОК 6, ПК.3.5)***
10. Какова роль криптографической защиты информации в системе ТЗИ? ***(оцениваемые знания, умения, компетенции З 5, З 7, У 2, ОК 8, ПК.3.1)***
11. Какие угрозы могут возникнуть при использовании компьютерных сетей и как их можно предотвратить с помощью ТЗИ? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 3, ОК 7, ПК.3.2)***
12. Какие организационные меры применяются для повышения уровня ТЗИ? ***(оцениваемые знания, умения, компетенции З 7, З 7, У 4, ОК 3, ПК.3.5)***
13. Какие современные технологии используются для обнаружения и предотвращения технических каналов утечки информации? ***(оцениваемые знания, умения, компетенции З 6, З 9, У 1, ОК 10, ПК.3.3)***
14. Каков порядок проведения оценки эффективности мер по ТЗИ? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 5, ОК 3, ПК.3.4)***
15. Как связаны между собой ТЗИ и физическая безопасность объектов информатизации? ***(оцениваемые знания, умения, компетенции З 4, З 7, У 1, ОК 2, ПК.3.5)***

Тема 1.2. Общие положения защиты информации техническими средствами

Вопросы:

1. Что понимается под защитой информации техническими средствами? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 1, ОК 7, ПК.3.5)***
2. Какие основные категории средств защиты информации выделяются? ***(оцениваемые знания, умения, компетенции З 2, З 8, У 6, ОК 3, ПК.3.4)***
3. Как классифицируются технические средства защиты информации по

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

4. В чем заключаются особенности использования программно-аппаратных комплексов для защиты информации? ***(оцениваемые знания, умения, компетенции З 3, З 8, У 4, ОК 5, ПК.3.3)***
5. Каким образом осуществляется интеграция технических средств защиты информации в существующую информационную систему? ***(оцениваемые знания, умения, компетенции З 4, З 7, У 3, ОК 4, ПК.3.1)***
6. Какие нормативные акты и стандарты регулируют использование технических средств защиты информации в РФ? ***(оцениваемые знания, умения, компетенции З 5, З 6, У 2, ОК 7, ПК.3.2)***
7. Как обеспечивается совместимость различных технических средств защиты информации в рамках одной системы? ***(оцениваемые знания, умения, компетенции З 5, З 9, У 1, ОК 6, ПК.3.3)***
8. Какие преимущества имеет использование автоматизированных систем управления защитой информации? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 3, ОК 8, ПК.3.5)***
9. Какими способами осуществляется тестирование и оценка эффективности технических средств защиты информации? ***(оцениваемые знания, умения, компетенции З 2, З 7, У 4, ОК 2, ПК.3.4)***
10. Какие проблемы могут возникать при эксплуатации технических средств защиты информации? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 6, ОК 9, ПК.3.3)***
11. Как осуществляется техническое обслуживание и модернизация средств защиты информации? ***(оцениваемые знания, умения, компетенции З 3, З 5, У 2, ОК 10, ПК.3.5)***
12. Каковы перспективы развития технических средств защиты информации в будущем? ***(оцениваемые знания, умения, компетенции З 3, З 7, У 3, ОК 1, ПК.3.1)***

Раздел 2. Теоретические основы инженерно-технической защиты информации
Тема 2.1. Информация как предмет защиты

Вопросы:

1. Что такое информация с точки зрения защиты данных? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 5, ПК.3.5)***
2. Какие виды информации подлежат защите? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 2, ОК 1, ПК.3.1)***
3. Чем определяется ценность информации? ***(оцениваемые знания,***

умения, компетенции З 1, З 9, У 6, ОК 1, ПК.3.5)

4. Какие угрозы могут воздействовать на информацию? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 4, ОК 6, ПК.3.5)***
5. Как различаются угрозы в зависимости от источника возникновения? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 3, ОК 4, ПК.3.2)***
6. Какие меры принимаются для защиты информации от несанкционированного доступа? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 2, ОК 1, ПК.3.5)***
7. Как обеспечивается целостность информации? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 1, ОК 7, ПК.3.5)***
8. Почему конфиденциальность является важным аспектом защиты информации? ***(оцениваемые знания, умения, компетенции З 1, З 5, У 4, ОК 3, ПК.3.3)***
9. Как осуществляется классификация информации по уровню секретности? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 5, ОК 8, ПК.3.4)***
10. Какие правовые нормы регулируют защиту информации в Российской Федерации? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 1, ОК 2, ПК.3.5)***
11. Каковы последствия нарушения защиты информации? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 6, ОК 9, ПК.3.5)***
12. Какие современные технологии используются для защиты информации? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 1, ПК.3.1)***
13. Как оценивается эффективность мер по защите информации? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 4, ОК 10, ПК.3.3)***

Тема 2.2. Технические каналы утечки информации

Вопросы:

1. Что такое технические каналы утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 1, ПК.3.5)***
2. Какие основные виды технических каналов утечки информации существуют? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 2, ОК 5, ПК.3.2)***
3. Как образуются акустические каналы утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 1, ОК 3, ПК.3.5)***

4. Какие меры принимаются для защиты информации от утечек через электромагнитные каналы? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 6, ОК 4, ПК.3.1)***
5. Как влияет дистанционное наблюдение на возникновение визуальных каналов утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 1, ОК 1, ПК.3.2)***
6. Какие устройства могут использоваться злоумышленниками для перехвата информации через побочные электромагнитные излучения и наводки (ПЭМИН)? ***(оцениваемые знания, умения, компетенции З 1, З 5, У 8, ОК 2, ПК.3.5)***
7. Как осуществляется защита информации от утечек через сети связи? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 5, ОК 10, ПК.3.5)***
8. Какие угрозы возникают при использовании беспроводных сетей и как они предотвращаются? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 1, ОК 1, ПК.3.3)***
9. Каким образом защищаются информационные системы от утечек через физические каналы (например, хищение носителей информации)? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 3, ОК 8, ПК.3.5)***
10. Какие современные технологии используются для выявления и предотвращения технических каналов утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 2, ОК 7, ПК.3.5)***
11. Как проводится анализ рисков, связанных с техническими каналами утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 6, ПК.3.4)***
12. Какие нормативно-правовые акты регулируют защиту информации от технических каналов утечки в Российской Федерации? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 4, ОК 1, ПК.3.5)***
13. Как оценивается эффективность мер по защите от технических каналов утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 1, ОК 5, ПК.3.5)***

Тема 2.3. Методы и средства технической разведки

Вопросы:

1. Что такое техническая разведка и какие цели она преследует? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 6, ОК 4, ПК.3.1)***
2. Какие основные методы технической разведки существуют?

(оцениваемые знания, умения, компетенции З 1, З 9, У 1, ОК 8, ПК.3.5)

3. Какие средства используются для осуществления технической разведки? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 5, ОК 9, ПК.3.4)***
4. Как осуществляется перехват информации с помощью радиотехнических средств? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 4, ОК 4, ПК.3.5)***
5. Какие методы используются для получения информации через компьютерные сети? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 1, ОК 1, ПК.3.5)***
6. Как применяется видеонаблюдение и аудиозапись в технической разведке? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 3, ОК 3, ПК.3.3)***
7. Какие современные технологии используются для сбора информации через мобильные устройства? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 2, ОК 1, ПК.3.2)***
8. Какие меры принимаются для защиты информации от технической разведки? ***(оцениваемые знания, умения, компетенции З 1, З 5, У 1, ОК 2, ПК.3.5)***
9. Как проводится анализ рисков, связанных с технической разведкой? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 3, ОК 1, ПК.3.5)***
10. Какие нормативно-правовые акты регулируют деятельность в области технической разведки в Российской Федерации? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 6, ОК 1, ПК.3.1)***
11. Как оценивается эффективность мер по защите от технической разведки? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 1, ОК 9, ПК.3.5)***
12. Какие перспективы развития методов и средств технической разведки вы видите в будущем? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 2, ОК 10, ПК.3.5)***
13. Поделитесь своими прогнозами относительно будущего развития технической разведки. ***(оцениваемые знания, умения, компетенции З 1, З 9, У 1, ОК 1, ПК.3.4)***

Раздел 3. Физические основы технической защиты информации

Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок

Вопросы:

1. Что такое технический канал утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 6, ОК 10, ПК.3.1)***
2. Какие основные виды технических каналов утечки информации существуют? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 1, ПК.3.5)***
3. Каковы механизмы образования акустических каналов утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 5, ОК 9, ПК.3.5)***
4. Какие меры принимаются для защиты информации от утечек через электромагнитные каналы? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 1, ОК 2, ПК.3.2)***
5. Как влияет дистанционное наблюдение на возникновение визуальных каналов утечки информации? ***(оцениваемые знания, умения, компетенции З 5, З 9, У 4, ОК 1, ПК.3.5)***
6. Какие устройства могут использоваться злоумышленниками для перехвата информации через побочные электромагнитные излучения и наводки (ПЭМИН)? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 5, ОК 1, ПК.3.3)***
7. Приведите примеры устройств и методов перехвата ПЭМИН. ***(оцениваемые знания, умения, компетенции З 1, З 8, У 1, ОК 2, ПК.3.5)***
8. Как осуществляется защита информации от утечек через сети связи? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 6, ОК 1, ПК.3.4)***
9. Какие угрозы возникают при использовании беспроводных сетей и как они предотвращаются? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 9, ПК.3.5)***
10. Каким образом защищаются информационные системы от утечек через физические каналы (например, хищение носителей информации)? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 1, ОК 3, ПК.3.2)***
11. Какие современные технологии используются для выявления и предотвращения технических каналов утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 5, У 2, ОК 1, ПК.3.4)***
12. Как проводится анализ рисков, связанных с техническими каналами утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 3, ОК 4, ПК.3.5)***

13. Какие нормативно-правовые акты регулируют защиту информации от технических каналов утечки в Российской Федерации? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 1, ОК 8, ПК.3.2)***
14. Как оценивается эффективность мер по защите от технических каналов утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 4, ОК 1, ПК.3.5)***

Тема 3.2. Физические процессы при подавлении опасных сигналов

Вопросы:

1. Что такое опасные сигналы и почему их необходимо подавлять? ***(оцениваемые знания, умения, компетенции З 8, З 9, У 2, ОК 1, ПК.3.3)***
2. Какие физические процессы лежат в основе подавления опасных сигналов? ***(оцениваемые знания, умения, компетенции З 5, З 4, У 1, ОК 7, ПК.3.5)***
3. Какие методы подавления опасных сигналов существуют? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 6, ОК 6, ПК.3.5)***
4. Как работают фильтры низких частот при подавлении опасных сигналов? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 1, ПК.3.2)***
5. Как работает экранирование при подавлении опасных сигналов? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 2, ОК 5, ПК.3.5)***
6. Какие материалы используются для создания экранов и почему? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 1, ОК 1, ПК.3.1)***
7. Как происходит подавление электромагнитных помех? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 3, ОК 1, ПК.3.5)***
8. Как используется заземление для снижения уровня опасных сигналов? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 1, ОК 2, ПК.3.2)***
9. Как влияют внешние условия на эффективность подавления опасных сигналов? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 4, ОК 1, ПК.3.5)***
10. Какие измерительные приборы используются для контроля качества подавления опасных сигналов? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 2, ОК 1, ПК.3.3)***
11. Какие существуют ограничения и трудности при подавлении опасных

сигналов? ***(оцениваемые знания, умения, компетенции З 4, З 5, У 6, ОК 3, ПК.3.5)***

12. Как развивается технология подавления опасных сигналов? ***(оцениваемые знания, умения, компетенции З 2, З 3, У 1, ОК 1, ПК.3.5)***
13. Каковы перспективы дальнейшего улучшения методов подавления опасных сигналов? ***(оцениваемые знания, умения, компетенции З 5, З 9, У 1, ОК 4, ПК.3.4)***

Раздел 4. Системы защиты от утечки информации

Тема 4.1. Системы защиты от утечки информации по акустическому каналу

Вопросы:

1. Что такое акустический канал утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 2, ОК 10, ПК.3.1)***
2. Какие основные источники акустической информации могут быть использованы для утечки? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 1, ОК 1, ПК.3.5)***
3. Какие методы используются для перехвата акустической информации? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 3, ОК 2, ПК.3.5)***
4. Каковы основные компоненты систем защиты от утечки информации по акустическому каналу? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 1, ПК.3.2)***
5. Какие технические средства используются для подавления акустического сигнала? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 6, ОК 9, ПК.3.5)***
6. Как работает система активного шумоподавления? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 1, ОК 1, ПК.3.4)***
7. Какие меры принимаются для защиты помещений от прослушивания? ***(оцениваемые знания, умения, компетенции З 4, З 5, У 5, ОК 1, ПК.3.5)***
8. Как производится оценка эффективности систем защиты от утечки информации по акустическому каналу? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 1, ОК 3, ПК.3.5)***
9. Какие нормативные документы регламентируют установку и эксплуатацию систем защиты от утечки информации по акустическому каналу? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 4, ОК 7, ПК.3.5)***
10. Каковы современные тенденции в развитии систем защиты от утечки

информации по акустическому каналу? ***(оцениваемые знания, умения, компетенции З 7, З 8, У 3, ОК 8, ПК.3.3)***

11. Какие сложности могут возникнуть при установке и настройке систем защиты от утечки информации по акустическому каналу? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 6, ПК.3.1)***
12. Как выбрать подходящую систему защиты от утечки информации по акустическому каналу для конкретного объекта? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 2, ОК 4, ПК.3.5)***
13. Как осуществляется техническое обслуживание и обновление систем защиты от утечки информации по акустическому каналу? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 3, ОК 5, ПК.3.2)***

Тема 4.2. Системы защиты от утечки информации по проводному каналу
Вопросы:

1. Что такое проводной канал утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 2, ОК 3, ПК.3.4)***
2. Какие основные виды проводных каналов утечки информации существуют? ***(оцениваемые знания, умения, компетенции З 1, З 5, У 4, ОК 1, ПК.3.5)***
3. Какие методы используются для перехвата информации по проводным каналам? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 1, ОК 10, ПК.3.5)***
4. Каковы основные компоненты систем защиты от утечки информации по проводному каналу? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 3, ОК 9, ПК.3.3)***
5. Какие технические средства используются для защиты информации от утечки по проводам? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 5, ОК 1, ПК.3.5)***
6. Как работает система экранирования кабелей? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 6, ОК 2, ПК.3.2)***
7. Какие меры принимаются для защиты линий связи от несанкционированного подключения? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 3, ПК.3.5)***
8. Как производится оценка эффективности систем защиты от утечки информации по проводному каналу? ***(оцениваемые знания, умения, компетенции З 2, З 3, У 2, ОК 8, ПК.3.5)***
9. Какие нормативные документы регламентируют установку и

эксплуатацию систем защиты от утечки информации по проводному каналу? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 4, ОК 1, ПК.3.1)***

10. Каковы современные тенденции в развитии систем защиты от утечки информации по проводному каналу? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 4, ОК 7, ПК.3.5)***
11. Какие сложности могут возникнуть при установке и настройке систем защиты от утечки информации по проводному каналу? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 1, ОК 6, ПК.3.1)***
12. Как выбрать подходящую систему защиты от утечки информации по проводному каналу для конкретного объекта? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 5, ОК 5, ПК.3.5)***
13. Как осуществляется техническое обслуживание и обновление систем защиты от утечки информации по проводному каналу? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 5, ОК 4, ПК.3.3)***

Тема 4.3. Системы защиты от утечки информации по вибрационному каналу

Вопросы:

1. Что такое вибрационный канал утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 2, ОК 9, ПК.3.5)***
2. Какие основные источники вибрации могут привести к утечке информации? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 1, ОК 10, ПК.3.1)***
3. Какие методы используются для перехвата информации по вибрационным каналам? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 1, ПК.3.5)***
4. Каковы основные компоненты систем защиты от утечки информации по вибрационному каналу? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 2, ОК 2, ПК.3.4)***
5. Какие технические средства используются для защиты информации от утечки по вибрациям? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 1, ОК 4, ПК.3.5)***
6. Как работает система демпфирования вибраций? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 3, ОК 3, ПК.3.5)***
7. Какие меры принимаются для защиты помещений от утечки информации по вибрациям? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 6, ОК 5, ПК.3.3)***
8. Как производится оценка эффективности систем защиты от утечки информации по вибрационному каналу? ***(оцениваемые знания, умения,***

компетенции З 1, З 4, У 5, ОК 9, ПК.3.5)

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

Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу

Вопросы:

1. Что такое электромагнитный канал утечки информации? ***(оцениваемые знания, умения, компетенции З 3, З 7, У 2, ОК 2, ПК.3.3)***
2. Какие основные источники электромагнитных излучений могут привести к утечке информации? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 1, ПК.3.5)***
3. Какие методы используются для перехвата информации по электромагнитным каналам? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 10, ПК.3.5)***
4. Каковы основные компоненты систем защиты от утечки информации по электромагнитному каналу? ***(оцениваемые знания, умения, компетенции З 3, З 4, У 6, ОК 3, ПК.3.5)***
5. Какие технические средства используются для защиты информации от утечки по электромагнитным излучениям? ***(оцениваемые знания, умения, компетенции З 5, З 9, У 3, ОК 9, ПК.3.4)***
6. Как работает система экранирования помещений? ***(оцениваемые знания, умения, компетенции З 7, З 8, У 4, ОК 8, ПК.3.5)***

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

Тема 4.5. Системы защиты от утечки информации по телефонному каналу

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)***

Тема 4.6. Системы защиты от утечки информации по электросетевому каналу

Вопросы:

1. Что такое электросетевой канал утечки информации? ***(оцениваемые знания, умения, компетенции З 3, З 9, У 6, ОК 5, ПК.3.2)***
2. Какие основные источники утечки информации по электросети 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 электросетевым каналам? ***(оцениваемые знания, умения, компетенции З 4, З 8, У 2, ОК 4, ПК.3.5)***
4. Каковы основные компоненты систем защиты от утечки информации по

электросетевому каналу? ***(оцениваемые знания, умения, компетенции З 5, З 7, У 1, ОК 1, ПК.3.4)***

5. Какие технические средства используются для защиты информации от утечки по электросети? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 3, ОК 2, ПК.3.5)***
6. Как работает система фильтрации высокочастотных сигналов в электросети? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 4, ОК 1, ПК.3.3)***
7. Какие меры принимаются для защиты электропитания от утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 1, ОК 3, ПК.3.5)***
8. Как производится оценка эффективности систем защиты от утечки информации по электросетевому каналу? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 5, ОК 10, ПК.3.5)***
9. Какие нормативные документы регламентируют установку и эксплуатацию систем защиты от утечки информации по электросетевому каналу? ***(оцениваемые знания, умения, компетенции З 1, З 5, У 1, ОК 6, ПК.3.1)***
10. Каковы современные тенденции в развитии систем защиты от утечки информации по электросетевому каналу? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 6, ОК 7, ПК.3.2)***
11. Какие сложности могут возникнуть при установке и настройке систем защиты от утечки информации по электросетевому каналу? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 4, ОК 1, ПК.3.5)***
12. Как выбрать подходящую систему защиты от утечки информации по электросетевому каналу для конкретного объекта? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 5, ОК 8, ПК.3.3)***
13. Как осуществляется техническое обслуживание и обновление систем защиты от утечки информации по электросетевому каналу? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 2, ОК 9, ПК.3.4)***

Тема 4.7. Системы защиты от утечки информации по оптическому каналу

Вопросы:

1. Что такое оптический канал утечки информации? ***(оцениваемые знания, умения, компетенции З 1, З 9, У 3, ОК 9, ПК.3.1)***
2. Какие основные источники утечки информации по оптическим каналам 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 оптическим каналам? ***(оцениваемые знания, умения, компетенции З 1, З 3, У 2, ОК 1, ПК.3.3)***
4. Каковы основные компоненты систем защиты от утечки информации по оптическому каналу? ***(оцениваемые знания, умения, компетенции З 1, З 8, У 5, ОК 8, ПК.3.5)***
5. Какие технические средства используются для защиты информации от утечки по оптическим каналам? ***(оцениваемые знания, умения, компетенции З 1, З 7, У 1, ОК 7, ПК.3.2)***
6. Как работает система зашифровки данных в волоконно-оптических линиях связи? ***(оцениваемые знания, умения, компетенции З 1, З 4, У 6, ОК 2, ПК.3.5)***
7. Какие меры принимаются для защиты волоконно-оптических линий связи от несанкционированного доступа? ***(оцениваемые знания, умения, компетенции З 1, З 6, У 2, ОК 6, ПК.3.2)***
8. Как производится оценка эффективности систем защиты от утечки информации по оптическому каналу? ***(оцениваемые знания, умения, компетенции З 1, З 5, У 1, ОК 3, ПК.3.5)***
9. Какие нормативные документы регламентируют установку и эксплуатацию систем защиты от утечки информации по оптическому каналу? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 3, ОК 5, ПК.3.4)***
10. Каковы современные тенденции в развитии систем защиты от утечки информации по оптическому каналу? ***(оцениваемые знания, умения, компетенции З 6, З 9, У 4, ОК 1, ПК.3.5)***
11. Какие сложности могут возникнуть при установке и настройке систем защиты от утечки информации по оптическому каналу? ***(оцениваемые знания, умения, компетенции З 4, З 5, У 1, ОК 4, ПК.3.3)***
12. Как выбрать подходящую систему защиты от утечки информации по оптическому каналу для конкретного объекта? ***(оцениваемые знания, умения, компетенции З 3, З 6, У 1, ОК 3, ПК.3.1)***
13. Как осуществляется техническое обслуживание и обновление систем защиты от утечки информации по оптическому каналу? ***(оцениваемые знания, умения, компетенции З 1, З 2, У 1, ОК 2, ПК.3.2)***

Раздел 5. Применение и эксплуатация технических средств защиты информации

Тема 5.1. Применение технических средств защиты информации

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 5.2. Эксплуатация технических средств защиты информации

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.03.01 Техническая защита информации

Специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

семестр 6 курс 3

группа 841

Билет № **1**

1.Предмет и задачи технической защиты информации.
2. Выявить и указать потенциальные каналы утечки информации в помещении банка. Указать причины возникновения каналов утечки информации. Описать методы подавления, выявленных каналов утечки информации.

Преподаватель: _____ Е.В. Зюбан
(подпись)

3.1. Перечень вопросов.

1. Предмет и задачи технической защиты информации. ***(оцениваемые знания, умения, компетенции: З 1, З 4, У 4, ОК 10, ПК. 3.1, ПК.3.2)***
2. Характеристика инженерно-технической защиты информации ***(оцениваемые знания, умения, компетенции: З 2, З 4, У 1, ОК 1, ПК. 3.1, ПК.3.3)***
3. Задачи и требования к способам и средствам защиты информации***(оцениваемые знания, умения, компетенции: З 1, З 5, У 4, ОК 2, ПК. 3.1, ПК.3.4)***
4. Классификация способов и средств защиты информации. ***(оцениваемые знания, умения, компетенции: З 2, З 6, У 2, ОК 2, ПК. 3.1, ПК.3.5)***
5. Особенности информации как предмета защиты. ***(оцениваемые знания, умения, компетенции: З 3, З 7, У 3, ОК 10, ПК. 3.1, ПК.3.5)***
6. Демаскирующие признаки объектов наблюдения, сигналов и веществ. ***(оцениваемые знания, умения, компетенции: З 1, З 4, У 5, ОК 7, ПК. 3.1, ПК.3.2)***
7. Понятие и особенности утечки информации. ***(оцениваемые знания, умения, компетенции: З 4, З 8, У 6, ОК 9, ПК. 3.1, ПК.3.4)***
8. Классификация каналов утечки информации. ***(оцениваемые знания,***

умения, компетенции: З 5, З 9, У 2, ОК 1, ПК. 3.4, ПК.3.5)

9. Классификация технических средств разведки. ***(оцениваемые знания, умения, компетенции: З 1, З 4, У 4, ОК 8, ПК. 3.1, ПК.3.2)***
10. Средства несанкционированного доступа к информации. ***(оцениваемые знания, умения, компетенции: З 2, З 4, У 1, ОК 4, ПК. 3.1, ПК.3.3)***
11. Физические основы побочных электромагнитных излучений и наводок. ***(оцениваемые знания, умения, компетенции: З 3, З 4, У 5, ОК 5, ПК. 3.1, ПК.3.4)***
12. Номенклатура и характеристика аппаратуры. ***(оцениваемые знания, умения, компетенции: З 1, З 5, У 5, ОК 6, ПК. 3.1, ПК.3.4)***
13. Скрытие речевой информации в каналах связи. ***(оцениваемые знания, умения, компетенции: З 1, З 6, У 5, ОК 3, ПК. 3.1, ПК.3.2)***
14. Подавление опасных сигналов акустоэлектрических преобразований. ***(оцениваемые знания, умения, компетенции: З 1, З 7, У 6, ОК 7, ПК. 3.1, ПК.3.2)***
15. Технические средства акустической разведки. ***(оцениваемые знания, умения, компетенции: З 1, З 7, У 6, ОК 8, ПК. 3.3, ПК.3.5)***
16. Номенклатура применяемых средств защиты информации***(оцениваемые знания, умения, компетенции: З 1, З 8, У 4, ОК 2, ПК. 3.4, ПК.3.5)***
17. Использование коммуникаций в качестве соединительных проводов.
18. Негласная запись информации на диктофоны. ***(оцениваемые знания, умения, компетенции: З 1, З 9, У 1, ОК 9, ПК. 3.1, ПК.3.2)***
19. Лазерные системы подслушивания. ***(оцениваемые знания, умения, компетенции: З 4, У 4, ОК 1, ПК. 3.3, ПК.3.4)***
20. Системы защиты информации от утечки по вибрационному каналу. ***(оцениваемые знания, умения, компетенции: З 3, З 4, У 1, ОК 10, ПК. 3.4, ПК.3.5)***
21. Прослушивание информации от радиотелефонов. ***(оцениваемые знания, умения, компетенции: З 5, З 9, У 1, ОК 1, ПК. 3.1, ПК.3.3)***
22. Системы защиты от утечки по электромагнитному каналу. ***(оцениваемые знания, умения, компетенции: З 6, З 7, У 2, ОК 2, ПК. 3.1, ПК.3.4)***
23. Контактный и бесконтактный методы съема информации. ***(оцениваемые знания, умения, компетенции: З 1, З 4, У 4, ОК 1, ПК. 3.1, ПК.3.5)***
24. Номенклатура применяемых средств защиты информации. ***(оцениваемые знания, умения, компетенции: З 2, З 5, У 3, ОК 3, ПК. 3.2, ПК.3.3)***
25. Низкочастотное устройство съема информации. ***(оцениваемые знания, умения, компетенции: З 3, З 5, У 6, ОК 5, ПК. 3.3, ПК.3.4)***

26. Высокочастотное устройство съема информации. ***(оцениваемые знания, умения, компетенции: З 4, З 6, У 4, ОК 4, ПК. 3.4, ПК.3.5)***
27. Телевизионные системы наблюдения. Приборы ночного видения. ***(оцениваемые знания, умения, компетенции: З 5, З 7, У 4, ОК 6, ПК. 3.1, ПК.3.2)***
28. Технические средства для уничтожения информации. ***(оцениваемые знания, умения, компетенции: З 1, З 8, У 6, ОК 7, ПК. 3.1, ПК.3.2)***
29. Проведение измерений параметров физических полей. ***(оцениваемые знания, умения, компетенции: З 1, З 9, У 5, ОК 8, ПК. 3.3, ПК.3.4)***
30. Этапы эксплуатации технических средств защиты информации. ***(оцениваемые знания, умения, компетенции: З 1, З 5, У 3, ОК 9, ПК. 3.1, ПК.3.3)***
31. Установка и настройка технических средств защиты информации. ***(оцениваемые знания, умения, компетенции: З 3, З 4, У 5, ОК 10, ПК. 3.1, ПК.3.5)***

3.2. Перечень практических заданий.

1. Выявить и описать потенциальные каналы утечки информации в помещениях (предприятия). Указать причины возникновения. Составить модель каналов утечки информации. ***(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. Для помещений (предприятия) определить основные источники информации и их носители. Классифицируйте и опишите категории помещений. ***(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. Представлены основные варианты возможной утечки речевой информации из объемов выделенных помещений (предприятия). Определите группы и виды каналов утечки. Опишите технические средства, с помощью которых может быть осуществлен перехват информации. Опишите возможные каналы утечки информации. ***(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. Опишите методы и средства технической защиты, которые могут применяться для блокирования угроз, связанных с утечкой информации (предприятия). ***(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. Для объекта защиты (предприятия) составьте список потенциальных угроз безопасности. ***(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. Составьте план защиты объекта (предприятия) с помощью технических средств. Поясните расположение и обоснуйте свой выбор. ***(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. Для объекта защиты (предприятия) выделите и опишите контролируемы зоны ОТСС. ***(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. Для помещения (объекта защиты) составить проект технической защиты информации от утечки по акустическому каналу. ***(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. Для помещения (объекта защиты) составить проект технической защиты информации от утечки по оптическому каналу. ***(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. Выявить и указать потенциальные каналы утечки информации в помещении (предприятия). Указать причины возникновения каналов утечки информации. Описать методы подавления, выявленных каналов утечки информации. ***(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/