Приложение ППССЗ по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем 2021-2022 уч.г.:
Комплект контрольно-оценочных средств по
ПМ 03. Защита информации техническими средствами

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

Комплект контрольно-оценочных средств

по

ПМ.03. Защита информации техническими средствами

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:
Гадяцкая И.Д. преподаватель ОГАПОУ «Алексеевский колледж»

СОДЕРЖАНИЕ

1. Паспорт комплекта оценочных средств

1.1. Область применения комплекта оценочных средств

В соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования (далее – ФГОС СПО) колледж самостоятельно планирует результаты обучения по ПМ 02. Защита информации техническими средствами, 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 ПМ 03. Защита информации техническими средствами**.**

КОС включают типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и практического опыта, характеризующих этапы формирования компетенций в процессе освоения образовательной программы для организации промежуточной аттестации в форме **экзамена по модулю**.

КОС разработан на основании рабочей программы ПМ 03. Защита информации техническими средствами.

1.2 Планируемые результаты освоения профессионального модуля:

Предметом оценки служат знания, умения и практический опыт, предусмотренные ФГОС СПО, направленные на формирование профессиональных компетенций.

Таблица 1

Наименование МДК и практик	Промежуточная аттестация	
	Форма контроля	Проверяемые компетенции/знания/умения/ практический опыт
МДК.03.01 Техническая защита информации	Экзаменационная работа	У1-У6, З1-З9, ПО1-ПО9, ОК 01-ОК 10, ПК 3.1.-ПК 3.5
МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации		У1-У6, З1-З9, ПО1-ПО9, ОК 01-ОК 10, ПК 3.1.-ПК 3.5
УП.03 Учебная практика		У1-У6, З1-З9, ПО1-ПО9, ОК 01-ОК 10, ПК 3.1.-ПК 3.5
ПП.03 Производственная практика		У1-У6, З1-З9, ПО1-ПО9, ОК 01-ОК 10, ПК 3.1.-ПК 3.5

В результате освоения профессионального модуля 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 профессионального модуля 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 профессионального модуля 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 профессионального модуля:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. 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 профессионального модуля:

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 профессионального модуля

Таблица 2

Код и наименование профессиональных и общих компетенций, формируемые в рамках междисциплинарного курса	Критерии оценки	Методы оценки
ПК 3.1 Осуществлять установку, монтаж, настройку и техническое обслуживание	Демонстрировать умения и практические навыки в установке, монтаже, настройке и проведении	Тестирование, экзамен экспертное наблюдение выполнения практических

технических средств защиты информации в соответствии с требованиями эксплуатационной документации	технического обслуживания технических средств защиты информации в соответствии с требованиями эксплуатационной документации	работ, оценка решения ситуационных задач
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, экзамен экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач
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, экзамен экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач
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, экзамен экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач
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, экзамен экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач

2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, характеризующих этапы формирования компетенций в процессе освоения профессионального модуля для организации промежуточной аттестации в форме экзамена

Раздел 1 модуля. Применение технической защиты информации МДК.03.01 Техническая защита 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.3.2)

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

Соотнесите понятия с их определениями.

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

Запишите ответ:

a	
b	
c	
d	

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

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

Расположите этапы разработки системы защиты информации в правильной последовательности.

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

Запишите ответ:

1	
2	

3	
4	
5	

Задание № 3 Задание на развернутый ответ
(оцениваемые практический опыт, знания, умения, компетенции ПО 6, ПО 7, ПО 8, ПО 9, З 6, З 7, У 5, У 6, ОК 1, ОК 5, ОК 6, ОК 7, ПК.3.4, 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 Задание на выбор одного ответа
(оцениваемые практический опыт, знания, умения, компетенции: ПО 5, ПО 6, ПО 9, З 1, З 2, З 8, З 9, У 3, У 4, У 6, ОК 4, ОК 10, ПК.3.5)
Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.
Вопрос: Что является основным принципом системного подхода при решении задач инженерно-технической защиты информации?
a) Минимизация затрат на реализацию проекта.
b) Учет всех взаимосвязей между элементами системы для достижения общей цели.
c) Максимальное упрощение процесса внедрения системы.
d) Использование самых современных технологий.
Запишите ответ: _____

Задание № 5 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 № 6. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.
(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, З 1, З 2,

З 8, У 1, У 4, ОК 3, ОК 4, ПК.3.5)

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

Соотнесите принципы системного анализа с их описаниями.

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

Запишите ответ:

a	
b	
c	
d	

Задание № 7 Прочитайте текст и установите последовательность. Ответ запишите в таблицу.

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

Расположите этапы системного анализа в правильном порядке.

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

Запишите ответ:

1	
2	
3	
4	
5	

Задание № 8 Задание на выбор одного ответа

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

Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

Вопрос: Какие задачи решает инженерно-техническая защита информации?

a) Повышение производительности труда.

b) Обеспечение конфиденциальности, целостности и доступности информации.

c) Улучшение эргономики рабочих мест.

d) Увеличение прибыли компании.

Задание № 9. 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 № 10 Прочитайте текст и установите последовательность. Ответ запишите в таблицу.

(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:

a) Выбор технических средств защиты
b) Оценка текущих рисков
c) Анализ требований к защите информации
d) Установка и настройка системы
e) Мониторинг и поддержка системы

Запишите ответ:

1	
2	
3	
4	
5	

Задание № 11 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 № 12 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 4ПК.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 № 13. 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.
Соотнесите понятия с их определениями.
Установите соответствие между физическими методами защиты информации и их описаниями:

Метод защиты	**Описание**
a) Экранирование	1) Замена оригинальных компонентов схемы устройствами, затрудняющими копирование информации.
b) Демонтаж элементов	2) Устройство, создающее препятствия для распространения электромагнитных волн.
c) Глушение	3) Удаление отдельных функциональных блоков или узлов устройства для предотвращения утечки информации.

Запишите ответ:

a	
b	
c	

Задание № 14 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 № 15 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 № 16 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,)
Расположите этапы установки системы защиты информации от утечки по акустическому каналу в правильной последовательности:
a) Установка звукоизолирующих материалов на стены и окна помещения.
b) Анализ потенциальных источников акустического сигнала (разговоры, работа техники).
c) Выбор подходящих технических средств для защиты.
d) Оценка эффективности установленной системы защиты.

Запишите ответ:

1	
2	
3	
4	

Задание № 17 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 № 18 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 № 19. 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**
a	Принцип работы микрофона и телефона	1. Меры и устройства для предотвращения несанкционированной аудиозаписи
b	Использование коммуникаций в качестве соединительных проводов	2.Передача данных через существующие коммуникационные сети
c	Негласная запись информации на диктофоны	3.Скрытая аудиозапись разговоров или других звуков
d	Системы защиты от диктофонов	4. Преобразование звуковых волн в электрические сигналы и обратно

Запишите ответ:

a	
b	
c	
d	

Задание № 20 Прочитайте текст и установите последовательность. Ответ запишите в таблицу.
(оцениваемые практический опыт, знания, умения, компетенции ПО 8, ПО 9, З 1, З 23

6У 1, У 2, У 5, ОК 1, ОК 2, ОК 6, ПК. 3.3, ПК.3.4,)

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

a) Установка экранирующих материалов на кабели и оборудование.

b) Анализ существующих коммуникационных сетей и выявление уязвимых мест.

c) Выбор подходящих технических средств для защиты.

d) Оценка эффективности установленной **системы защиты. Запишите ответ:**

1	
2	
3	
4	

Задание № 21 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 № 22 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 № 23. 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 № 24 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 № 25 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 № 26. Задание на выбор одного ответа
(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, З 5, З 6, З 7 У 3, У 4, У 5, ОК 4, ОК 5, ПК.3.5)

Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

Что из перечисленного является средством защиты от утечки информации по электромагнитному каналу?

a) Экранирующий материал
b) Радиозакладка
c) Детектор радиопередач
d) Приемник информации с радиозакладок

Запишите ответ: _____

Задание № 27 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 № 28. Задание на выбор одного ответа

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

Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

Что из перечисленного относится к номенклатуре средств защиты информации от несанкционированной утечки по электросетевому каналу?

a) Низкочастотное устройство съема информации
b) Высокочастотное устройство съема информации
c) Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу

Запишите ответ: _____

Задание № 29 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 № 30 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 № 31 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 № 32 Задание на выбор одного ответа

(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)

Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

Что из перечисленного относится к системам защиты информации по оптическому каналу?

a) Зеркальные стекла
b) Инфракрасные фильтры
c) Лазерные сканеры
d) Акустические экраны

Запишите ответ: _____

Задание № 33. 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 № 34 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 № 35 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

Ключи ответов

Номер задания	Ответ
1	a-1, b-3, c-2, d-4
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	b
5	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.
6	a-1, b-3, c-2, d-4
7	1, 2, 3, 4, 5
8	b
9	a-2, b-1, c-3
10	c → b → a → d → e
11	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.
12	b)
13	a-2, b-3, c-1
14	d → a → c → b
15	b) Блокировка USB-портов
16	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.
17	a-1, b-3, c-2, d-4, e-5
18	b →c → a → d
19	b) Прослушивание информации направленными микрофонами

20	a-4, b-2, c-3, d-1
21	b →c → a → d
22	c) Скрытая установка микрофона в офисе
23	a-4, b-2, c-3, d-1
24	b →c → a → d
25	**c) Гидроакустический преобразователь**
26	a) Экранирующий материал
27	f) Системы защиты от утечки по электромагнитному каналу.
28	c) Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.
29	a) Фильтры высоких частот
30	b) Камера видеонаблюдения.
31	b) Тепловизор.
32	b) Инфракрасные фильтры.
33	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
34	1 → 2 → 3 → 4
35	b) Блокировка USB-портов

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**
0-17 баллов	2 (неудовлетворительно)	0-50%	низкий
18-25 баллов	3 (удовлетворительно)	57-72%	базовый
26-30 баллов	4 (хорошо)	72-86%	повышенный
31-35 баллов	5 (отлично)	87-100%	высокий

Раздел 2 модуля. Применение инженерно-технических средств физической защиты объектов информатизации

МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

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

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

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

Соотнесите понятия с их определениями.

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

Запишите ответ:

a	
b	
c	
d	

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

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

Расположите этапы разработки системы защиты информации в правильной последовательности.

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

Запишите ответ:

1	
2	
3	
4	
5	

Задание № 3 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 Задание на выбор одного ответа

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

Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

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

a) Минимизация затрат на реализацию проекта.

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

c) Максимальное упрощение процесса внедрения системы.

d) Использование самых современных технологий.

Запишите ответ: _____

Задание № 5 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 № 6. В задании установите соответствие между понятием и его определением. Ответ запишите в таблицу.

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

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

Соотнесите принципы системного анализа с их описаниями.

Принцип	**Описание**
a) Целостность	1) Рассмотрение проблемы как части более широкой системы
b) Иерархичность	2) Учёт взаимозависимостей между различными аспектами проблемы

c) Многокритериальность	3) Возможность декомпозиции сложной системы на более простые компоненты
d) Динамичность	4) Изменчивость во времени, необходимость учёта изменений и адаптации системы

Запишите ответ:

a	
b	
c	
d	

Задание № 7 Прочитайте текст и установите последовательность. Ответ запишите в таблицу.

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

Расположите этапы системного анализа в правильном порядке.

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

Запишите ответ:

1	
2	
3	
4	
5	

Задание № 8 Задание на выбор одного ответа

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

Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

Вопрос: Какие задачи решает инженерно-техническая защита информации?

a) Повышение производительности труда.

b) Обеспечение конфиденциальности, целостности и доступности информации.

c) Улучшение эргономики рабочих мест.

d) Увеличение прибыли компании.

Задание № 9. 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 № 10 Прочитайте текст и установите последовательность. Ответ запишите в таблицу.

(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:

a) Выбор технических средств защиты
b) Оценка текущих рисков
c) Анализ требований к защите информации
d) Установка и настройка системы
e) Мониторинг и поддержка системы

Запишите ответ:

1	
2	
3	
4	
5	

Задание № 11 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 № 12 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 4ПК.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 № 13. 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.
Соотнесите понятия с их определениями.
Установите соответствие между физическими методами защиты информации и их описаниями:

Метод защиты	**Описание**
a) Экранирование	1) Замена оригинальных компонентов схемы устройствами, затрудняющими копирование информации.
b) Демонтаж элементов	2) Устройство, создающее препятствия для распространения электромагнитных волн.
c) Глушение	3) Удаление отдельных функциональных блоков или узлов устройства для предотвращения утечки информации.

Запишите ответ:

a	
b	
c	

Задание № 14 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 № 15 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 № 16 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 № 17. 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 № 18 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,)

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

a) Установка звукоизолирующих материалов на стены и окна помещения.

b) Анализ потенциальных источников акустического сигнала (разговоры, работа техники).

c) Выбор подходящих технических средств для защиты.

d) Оценка эффективности установленной системы защиты.

Запишите ответ:

1	
2	
3	
4	

Задание № 19 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 № 20 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 № 21. 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
a	Принцип работы микрофона и телефона	1. Меры и устройства для предотвращения несанкционированной аудиозаписи
b	Использование коммуникаций в качестве соединительных проводов	2.Передача данных через существующие коммуникационные сети
c	Негласная запись информации на диктофоны	3.Скрытая аудиозапись разговоров или других звуков
d	Системы защиты от диктофонов	4. Преобразование звуковых волн в электрические сигналы и обратно

Запишите ответ:

a	
b	
c	
d	

Задание № 22 Прочитайте текст и установите последовательность. Ответ запишите в таблицу.

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

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

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

1	
2	
3	
4	

Задание № 23 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 № 24. 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 № 25 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 № 26 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 № 27 Задание на выбор одного ответа
(оцениваемые практический опыт, знания, умения, компетенции: ПО 1, ПО 2, З 5, З 6, З 7 У 3, У 4, У 5, ОК 4, ОК 5, ПК.3.5)
Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.
Что из перечисленного является средством защиты от утечки информации по электромагнитному каналу?
a) Экранирующий материал
b) Радиозакладка
c) Детектор радиопередач
d) Приемник информации с радиозакладок
Запишите ответ: _____

Задание № 28 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 № 29 Задание на выбор одного ответа
(оцениваемые практический опыт, знания, умения, компетенции: ПО 3, ПО 4, З 4, З 5, У 4, У 5ОК 1, ОК 5, ОК 6, ПК.3.2,)
Выберите правильный вариант ответа и обведите кружочком номер правильного ответа.

Что из перечисленного относится к номенклатуре средств защиты информации от несанкционированной утечки по электросетевому каналу?

a) Низкочастотное устройство съема информации
b) Высокочастотное устройство съема информации
c) Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу
Запишите ответ: _____

Задание № 30 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 № 31 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 № 32 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 № 33. 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 № 34 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 № 35 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

Ключи ответов

Номер задания	Ответ
1	a-1, b-3, c-2, d-4
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	b
5	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.
6	a-1, b-3, c-2, d-4
7	1, 2, 3, 4, 5
8	b
9	a-2, b-1, c-3
10	c → b → a → d → e
11	Основные принципы инженерно-технической защиты информации включают: 1. Конфиденциальность: 2. Целостность: 3. Доступность:

	4. Аутентификация: 5. Журналирование и аудит:
12	b)
13	a-2, b-3, c-1
14	d → a → c → b
15	b) Блокировка USB-портов
16	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.
17	a-1, b-3, c-2, d-4, e-5
18	b →c → a → d
19	b) Прослушивание информации направленными микрофонами
20	a-4, b-2, c-3, d-1
21	b →c → a → d
22	c) Скрытая установка микрофона в офисе
23	a-4, b-2, c-3, d-1
24	b →c → a → d
25	**c) Гидроакустический преобразователь**
26	a) Экранирующий материал
27	f) Системы защиты от утечки по электромагнитному каналу.
28	c) Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.
29	a) Фильтры высоких частот

30	b) Камера видеонаблюдения.
31	b) Тепловизор.
32	b)
33	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
34	1 → 2 → 3 → 4
35	b) Блокировка USB-портов

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**
0-17 баллов	2 (неудовлетворительно)	0-50%	низкий
18-25 баллов	3 (удовлетворительно)	57-72%	базовый
26-30 баллов	4 (хорошо)	72-86%	повышенный
31-35 баллов	5 (отлично)	87-100%	высокий

2.2. Практикоориентированные задания

Задание № 1.

Текст задания.

Промышленное предприятие (условно ОАО «Маяк») специализируется на производстве пластмассовых труб, которые по своим качествам пользуются большим спросом. Охрана и защита коммерческих секретов, связанных с технологией производства труб, находятся в центре внимания руководства и службы безопасности предприятия. Предприятие имеет административную зону, где расположены управленческие структуры, производственную и складскую зоны. Все эти зоны разделены заборами. Предприятие имеет широкий круг партнеров, клиентов (в том числе и за рубежом). В сфере деятельности предприятия часто возникают конфликтные ситуации с конкурентами и спорные вопросы с органами местной власти по земельным и финансовым вопросам.

Инструкция.

1. Последовательность и условие выполнения задания:

Отчет должен содержать следующие скриншоты экранов:

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.

3. Разработайте и обоснуйте систему видеонаблюдения административной зоны.
Выполнение задания:
- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.
Подготовленный продукт
- разработанная система видеонаблюдения административной зоны;
- определение объектов и субъектов системы безопасности предприятия;
- определение видов охраны предприятия.
2. Дополнительные материалы, которыми может пользоваться обучающийся:
- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.
Максимальное время выполнения задания - 45 мин.

Задание 2.
Текст задания.
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.

Инструкция.
Последовательность и условие выполнения задания:
Отчет должен содержать следующие скриншоты экранов:
1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему видеонаблюдения административной зоны.
Выполнение задания:
- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.
2. Дополнительные материалы, которыми может пользоваться обучающийся:
- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.
Максимальное время выполнения задания - 45 мин.

Задание № 3

Текст задания

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.

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.

Инструкция.

Последовательность и условие выполнения задания:

Отчет должен содержать следующие скриншоты экранов:

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему видеонаблюдения административной зоны.

Выполнение задания:

- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.

2. Дополнительные материалы, которыми может пользоваться обучающийся:

- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.

Максимальное время выполнения задания - 45 мин.

Задание №4

Текст задания. 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

Инструкция.

Последовательность и условие выполнения задания:

Отчет должен содержать следующие скриншоты экранов:

1. Определите объекты и субъекты системы безопасности предприятия.

2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему видеонаблюдения административной зоны.
Выполнение задания:
- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.
2. Дополнительные материалы, которыми может пользоваться обучающийся:
- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.
Максимальное время выполнения задания - 45 мин.

Задание № 5
Текст задания. 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.
Инструкция.
Последовательность и условие выполнения задания:
Отчет должен содержать следующие скриншоты экранов:
1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему видеонаблюдения административной зоны.
Выполнение задания:
- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.
2. Дополнительные материалы, которыми может пользоваться обучающийся:
- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.
Максимальное время выполнения задания - 45 мин.

Задание № 6
Текст задания.
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

Инструкция.

Последовательность и условие выполнения задания:

Отчет должен содержать следующие скриншоты экранов:
1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему видеонаблюдения административной зоны.

Выполнение задания:
- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.

2. Дополнительные материалы, которыми может пользоваться обучающийся:
- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.

Максимальное время выполнения задания - 45 мин.

Задание №7

Текст задания

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

Инструкция.

Последовательность и условие выполнения задания:

Отчет должен содержать следующие скриншоты экранов:
1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему видеонаблюдения административной зоны.

Выполнение задания:
- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.

2. Дополнительные материалы, которыми может пользоваться обучающийся:
- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка

сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.
Максимальное время выполнения задания - 45 мин.

Задание № 7.
Текст задания
Вы являетесь инженером по защите информации в банке. Вам поручено разработать меры по защите информации от физического воздействия злоумышленников. Какие меры вы можете предложить? При решении задачи рассмотрите методы и средства перехвата информации
1.Принцип работы микрофона и телефона
2.Использование коммуникаций в качестве соединительных проводов
3.Негласная запись информации на диктофоны
4.Системы защиты от диктофонов
Инструкция.
Последовательность и условие выполнения задания:
Отчет должен содержать следующие скриншоты экранов:
1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему видеонаблюдения административной зоны.
Выполнение задания:
- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.
2. Дополнительные материалы, которыми может пользоваться обучающийся:
- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.
Максимальное время выполнения задания - 45 мин.

Задание № 8
Текст задания. 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, если у вас есть средства защиты:
1.Электронные стетоскопы
2.Лазерные системы подслушивания
3.Гидроакустические преобразователи
4.Системы защиты информации от утечки по вибрационному каналу

Инструкция.

Последовательность и условие выполнения задания:

Отчет должен содержать следующие скриншоты экранов:

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему видеонаблюдения административной зоны.

Выполнение задания:

- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.

2. Дополнительные материалы, которыми может пользоваться обучающийся:

- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.

Максимальное время выполнения задания - 45 мин.

Задание № 9

Текс задания. Вы являетесь специалистом по информационной безопасности в крупной компании. Руководство обратилось к вам с просьбой оценить риски утечки конфиденциальной информации по электромагнитному каналу в одном из помещений офиса. Опишите, какие шаги вы предпримете для решения этой задачи.

Методы 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

Инструкция.

Последовательность и условие выполнения задания:

Отчет должен содержать следующие скриншоты экранов:

1. Определите объекты и субъекты системы безопасности предприятия.
2. Выберите и обоснуйте виды охраны предприятия.
3. Разработайте и обоснуйте систему видеонаблюдения административной зоны.

Выполнение задания:

- ознакомление с заданием и планирование работы;
- соблюдение последовательности выполнения задания.

2. Дополнительные материалы, которыми может пользоваться обучающийся:

- ГОСТ 12.1.004-91 ССБТ. Пожарная безопасность.
- ГОСТ Р 51558-2014 «Средства и системы охранные телевизионные.
- Классификация. Общие технические требования. Методы испытаний».
- ГОСТ 12.4.026-2015. Межгосударственный стандарт. Система стандартов безопасности труда. Цвета сигнальные, знаки безопасности и разметка сигнальная. Назначение и правила применения. Общие технические требования и характеристики. Методы испытаний.

Максимальное время выполнения задания - 45 мин

Критерии оценивания практикоориентированных заданий

«5» «отлично» – студент показывает глубокое и полное овладение содержанием программного материала по профессиональному модулю, 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 профессиональному модулю, 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 профессиональному модулю, 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 профессиональному модулю, не умеет применять знания для решения практических и профессиональных задач, не демонстрирует овладение общими и профессиональными компетенциями и готовность к профессиональной деятельности.

3. Информационное обеспечение

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 информационной безопасности: В 2-х частях. Часть 2 Организационное обеспечение информационной безопасности: учеб. пособие. – М.: МИЭТ, 2013 – 172 с.

4. Организационно-правовое обеспечение Информационной 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 от 30 августа 2002 г. № 282.

24. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

25. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

26. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

27. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

28. 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.

29. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

30. 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

31. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

32. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

33. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

34. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

35. 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

36. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

37. 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

38. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

39. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

40. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

41. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

42. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

43. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

44. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

45. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.

46. Номенклатура показателей качества. Ростехрегулирование, 2005.

47. 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.

48. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

49. 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.

50. 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.

51. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.

52. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

53. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

54. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

55. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

56. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

57. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

58. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

59. 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. https://urait.ru/bcode/456793

2. 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. https://urait.ru/bcode/449548

3. 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.

4. Интерфейсы периферийных устройств – https://intuit.ru/studies/courses/92/92/lecture/28396

5. О компонентах системного блока — подробно – https://intuit.ru/studies/courses/3685/927/lecture/19564?page=2

6. Портативные компьютеры – https://intuit.ru/studies/courses/13910/1276/lecture/24146

7. Сравнительные характеристики процессоров – https://intuit.ru/studies/courses/15812/478/lecture/21074

8. Технические средства информационных технологий – https://intuit.ru/studies/courses/3481/723/lecture/14240

9. Устройства ввода информации – https://intuit.ru/studies/courses/3460/702/lecture/14158

10. Устройства вывода информации – https://intuit.ru/studies/courses/3460/702/lecture/14157

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 c. — 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/