МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)
Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

СПбГУТ))) Документ подписан простой электронной подписью

Сертификат: 00fd759708ffd39703
Владелец: Бачевский Сергей Викторович
Действителен с 15.03.2021 по 14.03.2026

УТВЕРЖДАЮ
Зам. директора по учебной работе
_____ О.В. Колбанева
21 апреля 2021 г.

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ С ИСПОЛЬЗОВАНИЕМ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ

(наименование профессионального модуля)

программа подготовки специалистов среднего звена

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем
(код и наименование специальности)

квалификация
техник по защите информации

Санкт-Петербург
2021

Комплект контрольно-оценочных средств составлен в соответствии с ППССЗ по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем и рабочей программой по учебной дисциплине «Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты»

Составитель:
Преподаватель _____ Н.В. Кривоносова
(подпись)

ОБСУЖДЕНО
на заседании предметной (цикловой) комиссии № 5 (информатики и программирования в компьютерных системах)
07 апреля 2021 г., протокол № 8

Председатель предметной (цикловой) комиссии:
_____Н.В. Кривоносова
(подпись)

ОДОБРЕНО

Методическим советом Санкт-Петербургского колледжа телекоммуникаций
21 апреля 2021 г., протокол № 6

Оглавление

1. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 4
1.1. Вид профессиональной деятельности 4
1.2. Матрица компетенций ПМ 03 7
2. ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ 10
2.1. Запланированные формы промежуточной аттестации по ПМ.03 10
3. ОЦЕНКА ОСВОЕНИЯ ТЕОРЕТИЧЕСКОГО КУРСА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ 11
3.1. Типовые задания для оценки освоения ПМ.03 19
3.1.1. Тестовые вопросы для промежуточной аттестации по Теме 1.1. Предмет и задачи технической защиты информации 19
3.1.2. Тестовые вопросы для промежуточной аттестации по Теме 1.2. Общие положения защиты информации техническими средствами 24
3.1.3. Тестовые вопросы для промежуточной аттестации по Теме 1.3. Технические каналы утечки информации 28
3.1.4. Тестовые вопросы для промежуточной аттестации по Теме 1.4. Методы и средства технической разведки 33
3.1.5. Тестовые вопросы для промежуточной аттестации по Теме 1.5. Физические основы утечки информации 37
3.1.6. Тестовые вопросы для промежуточной аттестации по Теме 1.6. Системы защиты от утечки информации 41
3.1.7. Тестовые вопросы для промежуточной аттестации по Теме 2.1. Цели и задачи физической защиты объектов информатизации 46
3.1.8. Тестовые вопросы для промежуточной аттестации по Теме 2.2. Общие сведения о комплексах инженерно-технических средств физической защиты 49
3.1.9. Тестовые вопросы для промежуточной аттестации по Теме 2.3. Система обнаружения комплекса инженерно-технических средств физической защиты 53
3.1.10. Тестовые вопросы для промежуточной аттестации по Теме 2.4. Система контроля управления доступом 57
3.1.11. Тестовые вопросы для промежуточной аттестации по Теме 2.5. Система телевизионного наблюдения 61
3.1.12. Тестовые вопросы для промежуточной аттестации по Теме 2.6. Система сбора, обработки, отображения и документирования информации 64
3.1.13. Тестовые вопросы для промежуточной аттестации по Теме 2.7. Система воздействия 68
3.1.14. Тестовые вопросы для промежуточной аттестации по Теме 2.8. Применение инженерно-технических средств физической защиты 70
3.1.15. Тестовые вопросы для промежуточной аттестации по Теме 2.9. Эксплуатация инженерно-технических средств защиты 74
3.1.16. Тестовые вопросы для промежуточной аттестации МДК 03.01 78
3.1.17. Тестовые вопросы для промежуточной аттестации МДК 03.02 94
3.2. Критерии оценок по типам (видам) заданий 104
3.3. Фонд оценочных средств для промежуточной аттестации по ПМ 03 108
I. ПАСПОРТ 108
II. ЗАДАНИЕ ДЛЯ ЭКЗАМЕНУЮЩЕГОСЯ 108
III. ПАКЕТ ЭКЗАМЕНАТОРА 109
III а. УСЛОВИЯ 109
III б. КРИТЕРИИ ОЦЕНКИ 109
4. ЛИСТ СОГЛАСОВАНИЯ 110

1. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Вид деятельности

Результатом освоения профессионального модуля является освоение вида деятельности «Защита информации в информационно телекоммуникационных системах и сетях с использованием технических средств защиты»:

В результате освоения программы профессионального модуля у обучающихся должны быть сформированы следующие компетенции, получены знания и развиты умения:

Таблица 1

Код компетенции	Содержание компетенции	Показатели оценки результата (знания, умения)
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Умения: – распознавать задачу и/или проблему в профессиональном и/или социальном контексте; – анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; – выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; – составить план действия; – определить необходимые ресурсы; – владеть актуальными методами работы в профессиональной и смежных сферах; – реализовать составленный план; – оценивать результат и последствия своих действий (самостоятельно или с помощью наставника). Знания: – актуальный профессиональный и социальный контекст, в котором приходится работать и жить; – основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; – алгоритмы выполнения работ в профессиональной и смежных областях; – методы работы в профессиональной и смежных сферах; – структуру плана для решения задач; – порядок оценки результатов решения задач профессиональной деятельности.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	Умения: – определять задачи для поиска информации; – определять необходимые источники информации; – планировать процесс поиска; – структурировать получаемую информацию; – выделять наиболее значимое в перечне информации; – оценивать практическую значимость результатов поиска; – оформлять результаты поиска. Знания:

		– номенклатура информационных источников, применяемых в профессиональной деятельности; – приемы структурирования информации; – формат оформления результатов поиска информации.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие	Умения: – определять актуальность нормативно-правовой документации в профессиональной деятельности; – выстраивать траектории профессионального и личностного развития Знания: – содержание актуальной нормативно-правовой документации; – современная научная и профессиональная терминология; – возможные траектории профессионального развития и самообразования
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	Умения: – организовывать работу коллектива и команды; – взаимодействовать с коллегами, руководством, клиентами. Знания: – психология коллектива; – психология личности; – основы проектной деятельности.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	Умения: – излагать свои мысли на государственном языке; – оформлять документы. Знания: – особенности социального и культурного контекста; правила оформления документов.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	Умения: – описывать значимость своей профессии; – презентовать структуру профессиональной деятельности по профессии (специальности). Знания: – сущность гражданско-патриотической позиции; – общечеловеческие ценности; правила поведения в ходе выполнения профессиональной деятельности.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	Умения: – соблюдать нормы экологической безопасности; – определять направления ресурсосбережения в рамках профессиональной деятельности по профессии (специальности). Знания: – правила экологической безопасности при ведении профессиональной деятельности; – основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения.
ОК 09	Использовать информационные технологии в	Умения: – применять средства информационных

	профессиональной деятельности	технологий для решения профессиональных задач; – использовать современное программное обеспечение. Знания: – современные средства и устройства информатизации; – порядок их применения и программное обеспечение в профессиональной деятельности.

Таблица 2

Код ПК	Наименование компетеции
ПК 3.1	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно – телекоммуникационных системах и сетях.
ПК 3.2	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно – телекоммуникационных системах и сетях.
ПК 3.3	Осуществлять защиту информации от утечки по техническим каналам в информационно – телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
ПК 3.4	Проводить отдельные работы по физической защите линий связи информационно – телекоммуникационных систем и сетей.

Таблица 3

Уметь:	
У-1	проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
У-2	проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам;
У-3	проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС;
У-4	проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
У-5	использовать средства физической защиты линий связи ИТКС;
У-6	применять нормативные правовые акты и нормативные методические документы в области защиты информации.
Знать:	
З-1	способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;
З-2	основные типы технических средств защиты информации от утечки по техническим каналам;
З-3	методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
З-4	организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;

З-5	порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;
З-6	содержание и организацию работ по физической защите линий связи ИТКС;
З-7	принципы действия и основные характеристики технических средств физической защиты;
З-8	законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности;
З-9	принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

В результате освоения программы профессионального модуля обучающийся должен иметь практический опыт:

Таблица 4

Практический опыт:	
ПО-1	установка, монтаж, настройка и испытания технических средств защиты информации от утечки по техническим каналам;
ПО-2	защита информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
ПО-3	проведение отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.

1.2. Матрица компетенций ПМ 03

Элемент КОС	**Проверяемые общие и профессиональные компетенции (знания, умения), практический опыт**																												
	ОК 01	ОК 02	ОК 03	ОК 04	ОК 05	ОК 06	ОК 07	ОК 09	У- 1	У- 2	У- 3	У- 4	У - 5	У- 6	З -1	З - 2	З - 3	З - 4	З - 5	З - 6	З - 7	З - 8	З - 9	ПО -1	ПО - 2	ПО - 3	ПК 3.1	ПК 3.2	ПК 3.3	ПК 3.4
МДК 03.01 Защита информации в ИТКС с использованием технических средств защиты																													
ЛР 1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ЛР 2	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ЛР 3	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ЛР 4	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ЛР 5	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ЛР 6	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ЛР 7	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ЛР 8	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ЛР 9	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ЛР 10	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ЛР 11	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ЛР 12	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ЛР 13	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	

ЛР 14	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ЛР 15	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ЛР 16	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 1	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 2	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 3	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 4	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 5	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 6	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 7	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПР 8	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 9	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 10	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 11	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 12	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 13	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 14	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 15	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 16	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 17	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 18	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
ПЗ 19	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	
МДК 03.02 Физическая защита линий связи ИТКС																													
ЛР 1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ЛР 2	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ЛР 3	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ЛР 4	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ЛР 5	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ЛР 6	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ЛР 7	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ЛР 8	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 2	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 3	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+

ПЗ 4	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 5	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 6	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 7	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 8	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 9	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 10	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 11	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 12	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 13	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 14	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 15	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 16	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 17	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 18	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 19	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 20	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 21	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 22	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 23	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 24	+	+	+	+	+	+	+	+	+	+	+	+		+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 25	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 26	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+
ПЗ 27	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+				+

Описание практических и лабораторных заданий см. – Методические указания по выполнению лабораторных заданий; Методические указания по выполнению практических заданий.

2. ФОРМЫ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

Обязательной формой аттестации по итогам освоения программы профессионального модуля являются дифференцированный зачет по МДК 03.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты, МДК 03.02 Физическая защита линий связи информационно-телекоммуникационных систем и сетей, прохождение учебной и производственной практик, экзамен (квалификационный). Результатом экзамена является однозначное решение: «вид деятельности освоен / не освоен».

2.1. Запланированные формы промежуточной аттестации по ПМ.03

Таблица 5

Элементы модуля, профессиональный модуль	**Формы промежуточной аттестации**
МДК 03.01	*Дифференцированный зачёт*
МДК 03.02	*Дифференцированный зачёт*
Учебная практика	*Дифференцированный зачёт*
Производственная практика	*Дифференцированный зачёт*
ПМ.03	*Экзамен*

3. ОЦЕНКА ОСВОЕНИЯ ТЕОРЕТИЧЕСКОГО КУРСА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Основной целью оценки курса профессионального модуля является оценка приобретенных умений, знаний и компетенций.

Оценка осуществляется с использованием следующих форм и методов контроля согласно п.2.6 и п.2.10 Положения о текущем контроле успеваемости обучающихся Санкт-Петербургского колледжа телекоммуникаций им. Э.Т. Кренкеля:

- *текущий контроль*
  - устный опрос на лекциях, практические и семинарские занятия;
  - практические задания;
  - самостоятельные работы;
  - контрольные работы;
  - защита лабораторных работ;
  - контроль самостоятельной работы (в письменной или устной форме);
  - тестирование (письменное или компьютерное);
- *рубежный контроль*
  - тестирование (письменное или компьютерное);
  - контрольные работы;
  - защита курсовых проектов (работ);
  - прием индивидуальных домашних заданий, рефератов, отчетов по лабораторным работам.

Текущий контроль обеспечивают выполнение видов работ на практике, освоение тем, выполнение лабораторных/практических работ, выполнение самостоятельных работ по МДК 03.01 и МДК 03.02.

Таблица 6

ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно-телекоммуникационных системах и сетях	
Иметь практический опыт:	***Виды работ на практике:***
– установка, монтаж, настройка и испытания технических средств защиты информации от утечки по техническим каналам; – защита информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;	– Монтаж различных типов датчиков. – Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. – Применение промышленных осциллографов, частотомеров и генераторов, и другого оборудования для защиты информации. – Рассмотрение системы контроля и управления доступом. – Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. – Рассмотрение датчиков периметра, их принципов работы. – Выполнение звукоизоляции помещений системы зашумления. – Реализация защиты от утечки по цепям электропитания и заземления. – Рассмотрение принципов работы ЛВП-10 Электромагнитный вибропреобразователь к ЛГШ-404 (для окон, стен, труб).

	– Рассмотрение многозонной системы обнаружения и блокирования мобильных средств связи для образовательных учреждений. – Монтаж различных типов датчиков. – Рассмотрение устройств обнаружения скрытых видеокамер «Алмаз». – Применение промышленных осциллографов, частотомеров и генераторов акустического шума, двухканального генератора, системы постановки виброакустических помех и другого оборудования для защиты информации.
Уметь:	***Тематика лабораторных/практических работ:***
– проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; – проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; – проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС; – проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; – использовать средства физической защиты линий связи ИТКС; – применять нормативные правовые акты и нормативные методические документы в области защиты информации.	– Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке. – Обоснование необходимости создания подсистемы технической защиты инфокоммуникационной системы на основе нормативных и методических документов. – Особенности утечки информации в проводных линиях связи. – Особенности утечки информации в беспроводных линиях связи. – Исследование уязвимостей и построение модели угроз объекта защиты. – Исследование возможностей системы оценки защищенности оптических линий связи. – Исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН. – Исследование возможностей системы оценки защищенности выделенных помещений. – Оценка защищенности информации по акустическому каналу. – Оценка защищенности информации по электромагнитному каналу.
Знать:	***Перечень тем, включенных в МДК:***
– способы защиты информации от утечки по техническим каналам с использованием технических средств защиты;	**Тема 1.1. Предмет и задачи технической защиты информации** **Тема 1.2. Общие положения защиты информации техническими средствами** **Тема 1.3. Технические каналы утечки информации**

– основные типы технических средств защиты информации от утечки по техническим каналам; – методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам; – организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам; – порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам; – содержание и организацию работ по физической защите линий связи ИТКС; – принципы действия и основные характеристики технических средств физической защиты; – законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности; – принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.	
Самостоятельная работа	работа с конспектами, литературой; подготовка отчетов практических работ
ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации используемых в информационно-телекоммуникационных системах и сетях ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями	
Иметь практический опыт:	***Виды работ на практике:***
– установка, монтаж, настройка и испытания технических средств защиты информации от утечки по техническим каналам;	– Рассмотрение системы контроля и управления доступом. – Рассмотрение принципов работы программно-аппаратного комплекса защиты объектов информационных

– защита информации по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;	технологий от разведки ПЭМИ, 0,009 - 1000 МГц. – Рассмотрение датчиков периметра, их принципов работы. – Изучение средств перехвата информации. – Микрофоны. – Акустические антенны. – Выбор типа микрофона и места его установки. – Изучение устройств подавления микрофонов. – Изучение устройств для перехвата речевой информации в проводных каналах. – Изучение оптико-акустической аппаратуры перехвата речевой информации. – Оптико-механические приборы. – Приборы ночного видения. – Средства скрытой фотосъемки.
Уметь:	***Тематика лабораторных/практических работ:***
– проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; – проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; – проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС; – проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; – использовать средства физической защиты линий связи ИТКС; – применять нормативные правовые акты и нормативные методические документы в области защиты информации.	– Определение каналов утечки ПЭМИН. – Работа с оборудованием по защите от утечки по ПЭМИН. – Работа с оборудованием по защите от утечки по ПЭМИН. – Определение утечки по цепям электропитания и заземления. – Защита от утечки по цепям электропитания и заземления. – Определение утечки информации по акустическому каналу. – Работа с оборудованием по защите от утечки по акустическому каналу. – Определение утечки информации по виброакустическому каналу. – Работа с оборудованием по защите от утечки по виброакустическому каналу. – Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации. – Поиск и локализация скрытых видеокамер. – Исследование методов защиты сотовых телефонов от несанкционированного прослушивания. – Исследование методов блокирования средств несанкционированного прослушивания и передачи данных различных стандартов.

	– Поиск устройств негласного съема информации с помощью профессионального нелинейного радиолокатора. – Инженерно-техническая защита информации. – Выявление и фиксация следов противоправной деятельности, связанной с использованием компьютерной деятельности. – Исследование уровня побочного электромагнитного излучения ПК. – Снятие диаграммы направленного микрофона. – Исследование спектра речевого сигнала. – Определение уровня побочного излучения в канале электросвязи. – Определение уровня побочного излучения в канале виброакустики. – Измерение уровня маскирующего виброакустического шума. – Измерение уровня маскирующего цифрового шума. – Испытание учебной аудитории на утечку информации по каналу ПЭМИН. – Испытание учебной аудитории на утечку информации по виброакустическому каналу.
Знать:	***Перечень тем, включенных в МДК:***
– способы защиты информации от утечки по техническим каналам с использованием технических средств защиты; – основные типы технических средств защиты информации от утечки по техническим каналам; – методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам; – организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам; – порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам;	**Тема 1.4. Методы и средства технической разведки** **Тема 1.5. Физические основы утечки информации** **Тема 1.6. Системы защиты от утечки информации**

– содержание и организацию работ по физической защите линий связи ИТКС; – принципы действия и основные характеристики технических средств физической защиты; – законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности; – принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.	
Самостоятельная работа	работа с конспектами, литературой; подготовка отчетов практических работ
ПК 3.4. Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей	
Иметь практический опыт:	***Виды работ на практике:***
– проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.	– Зоны подключения в линиях связи. – Перехват телефонных переговоров в зонах «А», «Б», «В», «Г», «Д», «Е». – Изучение перехвата сообщений в каналах сотовой связи. – Методы поиска закладных устройств как физических объектов и электронных средств. – Панорамные приемники. – Аппаратура контроля и защиты линии связи. – Средства создания акустических и электромагнитных маскирующих помех. – Измерение токов, напряжений и сопротивлений. – Исследование двухполюсников с помощью мультиметра. – Прямые и косвенные однократные измерения. – Обработка и представление однократных измерений при наличии систематической погрешности. – Стандартная обработка результатов прямых измерений с многократным наблюдением. – Обработка результатов прямых измерений с многократным наблюдением при наличии грубых погрешностей.

	– Определение погрешности цифрового вольтметра сличения и прямых измерений. – Измерение мощности и силы постоянного электромагнитного тока. – Измерение постоянного напряжения методом компенсации. – Измерение переменного электрического напряжения. – Измерение частоты и периода электрических сигналов. – Терморезисторные измерительные преобразователи. Измерители температуры. – Емкостные измерительные преобразователи. Измерение размера. – Индуктивные измерительные преобразователи. Измерение перемещения. – Термоэлектрические измерительные преобразователи. Измерение температуры. – Пьезоэлектрические измерительные преобразователи. Измерение переменных ускорений. – Изучение нормативных методических документов по обеспечению информационной безопасности техническими средствами. – Применение существующих способов выявления опасности целостности информации. – Выявление технических каналов утечки информации.
Уметь:	***Тематика лабораторных/практических работ:***
– проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; – проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; – проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых ИТКС; – проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; – использовать средства физической защиты линий связи ИТКС;	– Исследование возможностей СЗИ «Страж NT». – Исследование программной среды «Страж NT» – Управление пользователями «Страж NT», учет пользователей «Страж NT» – Избирательное управление «Страж NT» – Сортировка и поиск с «Страж NT» – Редактирование пользователей «Страж NT» – Изменение настроек «Страж NT» – Исследование возможностей «Сигурд М19» – Подготовка к работе «Сигурд М19» – Поиск сигналов ПЭМИН «Сигурд М19» – Анализ сигналов «Сигурд М19» – Обоснование необходимости создания СКУД объекта информатизации на основе нормативных и методических документов.

– применять нормативные правовые акты и нормативные методические документы в области защиты информации.	– Модели нарушителей физической безопасности объекта информатизации. – Разработка топологии многозональной и многорубежной системы физической защиты объекта. – Разработка структурной и функциональной схем СКУД. – Разработка основных организационных документов службы режима предприят**ия.** – Разработка методик контроля эффективности СКУД. – Рассмотрение принципов устройства, работы и применения средств видеонаблюдения. – Рассмотрение принципов устройства, работы и применения средств контроля доступа. – Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации. – Сравнение отечественных ССОИ. – Исследование возможностей радиолокатора NR-900EMS – Исследование возможностей прибора ST 033P Пиранья – Исследование возможностей анализатора спектра OSCOR Green – Проведение анализа защищаемой в кабинете руководителя информации. – Моделирование угроз воздействия на источники информации. – Разработка и осуществление мер по предотвращению проникновения злоумышленника к источникам информации. – Исследование возможностей имитатора АВРОРА-3 – Исследование возможностей комплекса КРОНА-ПРО – Исследование возможностей приемника СКОРПИОН-XL. – Исследование принципов работы индикатора поля РИЧ-8 – Исследование принципов работы индикатора поля MFP-8000. – Исследование принципов работы индикатора поля ST-107. – Исследование принципов работы индикатора поля PST-165. – Исследование возможностей системы ШЕПОТ.

Знать:	*Перечень тем, включенных в МДК:*
– способы защиты информации от утечки по техническим каналам с использованием технических средств защиты; – основные типы технических средств защиты информации от утечки по техническим каналам; – методики измерения параметров побочных электромагнитных излучений и наводок (далее – ПЭМИН), а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам; – организацию и содержание технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам; – порядок и правила ведения эксплуатационной документации на технические средства защиты информации от утечки по техническим каналам; – содержание и организацию работ по физической защите линий связи ИТКС; – принципы действия и основные характеристики технических средств физической защиты; – законодательство в области информационной безопасности, структуру государственной системы защиты информации, нормативных правовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности; – принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.	Тема 2.1. Цели и задачи физической защиты объектов информатизации Тема 2.2. Общие сведения о комплексах инженерно-технических средств физической защиты Тема 2.3. Система обнаружения комплекса инженерно-технических средств физической защиты Тема 2.4. Система контроля и управления доступом Тема 2.5. Система телевизионного наблюдения Тема 2.6. Система сбора, обработки, отображения и документирования информации Тема 2.7. Система воздействия Тема 2.8. Применение инженерно-технических средств физической защиты Тема 2.9. Эксплуатация инженерно-технических средств физической защиты
Самостоятельная работа	работа с конспектами, литературой; подготовка отчетов практических работ

3.1. Типовые задания для оценки освоения ПМ.03

Текущий контроль осуществляется за счет выполнения практических и самостоятельных работ, описание которых даны в методических рекомендациях по выполнению ЛПР по МДК 03.01 и МДК 03.02 и в методических рекомендациях по выполнению ВСР.

3.1.1. Тестовые вопросы для промежуточной аттестации по Теме 1.1. Предмет и задачи технической защиты информации

Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Как называется попытка реализации угрозы?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Непосредственная причина возникновения угрозы называется:	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Если злоумышленник внедрил в компьютер вредоносную программу и получил доступ к личной информации пользователя, какое свойство информации было нарушено?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 91	30
5	Как называется состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3	30

		ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
6	Если в результате DDOS-атаки новостной сайт на какое-то время вышел из строя и был недоступен для пользователей, какое свойство информации было нарушено?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Как называются методы защиты акустической информации, направленные на ослабление непосредственных акустических сигналов, циркулирующих в помещении?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Какой орган государственной власти осуществляет аттестацию объектов информатизации по требованиям безопасности?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	Как называются акустоэлектрические преобразователи, в которых под воздействием акустической волны возникают эквивалентные электрические сигналы?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Какой участник системы аттестации аттестует объекты информатизации по требованиям безопасности и выдает "Аттестаты соответствия"?	ПК 3.1 ПК 3.2 ПК 3.3	30

		ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	В случае формирования конфиденциальных документов с помощью информации, представленной на неконфиденциальных накопителях информации, неконфиденциальные накопители информации должны быть: 1. учтены в специальных журналах 2. отформатированы после обработки 3. открыты на запись 4. закрыты на запись	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Какой участник системы сертификации принимает решение о проведении повторной сертификации при изменениях в технологии изготовления и конструкции (составе) сертифицированных средств защиты информации: 1. федеральный орган по сертификации 2. центральный орган системы сертификации 3. орган по сертификации средств защиты информации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Нормативные правовые акты, затрагивающие права, свободы и обязанности человека относятся к: 1. конфиденциальной информации 2. государственной тайне 3. общедоступной информации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 93	30
4	Какой вид атаки направлен на получение конфиденциальной информации путем прослушивания сети? 1. анализ сетевого трафика 2. сканирование сети 3. навязывание ложного маршрута	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5	30

		ОК 6 ОК 7 ОК 9	
5	Как называется сигнал, который можно представить непрерывной функцией непрерывного аргумента? 1. Аналоговый 2. Дискретный 3. Импульсный	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	Подключение ЛВС к другой автоматизированной системе иного класса защищенности должно осуществляться с помощью: 1. Коммутатора 2. межсетевого экрана 3. маршрутизатора	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Как называются закладки, использующие для передачи информации силовые линии? 1. ИК-передатчики 2. сетевые закладки 3. радиозакладки	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Как называется признак защищаемого сигнала, позволяющий обнаруживать и распознавать его среди других сигналов? 1. Информационный 2. Основной 3. Демаскирующий	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	Установка аппаратного межсетевого экрана относится к: 1. организационным мерам обеспечения безопасности 2. техническим мерам обеспечения безопасности 3. физическим мерам обеспечения безопасности	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2	30

		ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
10	К основным показателям ТКУИ относятся: 1. длина канала 2. мощность 3. относительная информативность	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

3.1.2. Тестовые вопросы для промежуточной аттестации по Теме 1.2. Общие положения защиты информации техническими средствами

Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	Как называется совокупность информационных ресурсов, средств и систем информатизации, используемых в соответствии с заданной информационной технологией, и систем связи вместе с помещениями (транспортными средствами), в которых они установлены?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Как называется информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Как называется совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4	30

		ОК 5 ОК 6 ОК 7 ОК 9	
4	Какая организация курирует Банк данных угроз безопасности информации?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Как называются технические средства защиты, которые ослабляют уровень информативного сигнала?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств это…	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Как называется слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Как называется пространство, в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1	30

		ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
9	Как называется деятельность по разработке (ведению), утверждению, изменению (актуализации), отмене, опубликованию и применению документов по стандартизации и иная деятельность, направленная на достижение упорядоченности в отношении объектов стандартизации?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Как называется технический канал утечки информации, при котором производится съем информации с линии связи контактного подключения аппаратуры злоумышленника?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	В соответствии с каким документом осуществляется отнесение информации к государственной тайне? 1. ФЗ “Об информации, информационных технологиях и о защите информации” 2. ФЗ “О техническом регулировании” 3. ФЗ “О государственной тайне”	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Если автор статьи опубликовал ее в Интернете на сайте со свободным доступом, информацию из этой статьи можно отнести к: 1. конфиденциальной информации 2. государственной тайне 3. общедоступной информации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5	30

		ОК 6 ОК 7 ОК 9	
3	На кого возлагается ответственность за организацию работ по ТКЗИ в организации? 1. Отдел кадров 2. руководителя подразделения по защите информации 3. руководитель организации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Как называется комплекс административных и ограничительных мер, направленных на защиту информации путем регламентации деятельности персонала и порядка функционирования средств (систем)? 1. правовые меры защиты 2. организационные меры защиты 3. криптографические меры защиты	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Выделите организационные меры защиты информации от утечки по ТКУИ 1. определение границ контролируемой зоны 2. экранирование ОТСС 3. пространственное зашумление	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	В соответствии с ФЗ №149 "Об информации, информационных технологиях и о защите информации" информация разделяется на следующие категории: 1. общедоступная и конфиденциальная 2. общедоступная и ограниченного доступа 3. ограниченного доступа и государственная тайна	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Какой документ является основным нормативным документом в области регулирования в Российской Федерации? 1. Федеральный закон N 184 "О техническом регулировании" 2. Федеральный закон N 149 "Об информации, информационных технологиях и о защите информации"	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2	30

	3. Федеральный закон N 162 "О стандартизации в Российской Федерации"	ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
8	Кто осуществляет формирование требований к системе защиты информации конкретного объекта информатизации? 1. ФСБ 2. ФСТЭК 3. обладатель информации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	При входе в домен Windows пароль от учетной записи является… 1. средством идентификации 2. средством аутентификации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Как называется совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом? 1. система сертификации 2. система аккредитации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

3.1.3. Тестовые вопросы для промежуточной аттестации по Теме 1.3. Технические каналы утечки информации

Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	В каком техническом канале утечки информации в качестве носителей выступают электрические, электромагнитные и магнитные поля?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4	30

		ОК 5 ОК 6 ОК 7 ОК 9	
2	В каком техническом канале утечки информации в качестве носителей используются фотоны?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	В каком техническом канале утечки информации в качестве носителей используются упругие акустические волны?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Каналы, в которых утечка информации носит достаточно регулярный характер, называются:	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Как называются параметры сигнала, которые изменяются в зависимости от передаваемой информации?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	Как называется сигнал, который можно представить непрерывной функцией непрерывного аргумента?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1	30

		ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
7	Что такое φ в формуле $s(t) = Asin(2\pi ft + \varphi)$?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Сколько уровней амплитуды имеет бинарный сигнал?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым они были доверены по службе или стали известны в процессе работы, называется ...	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Перехват информации по прямому … каналу производится путем записи речевой информации диктофонами, установкой закладных устройств микрофонного типа, прослушиванием разговоров с помощью направленных микрофонов	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	Пропускная способность составного канала определяется как: 1. разность наибольшей и наименьшей пропускной способности входящих каналов 2. сумма наибольшей и наименьшей пропускной способности входящих каналов 3. наименьшая пропускная способность входящих каналов	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	К основным показателям ТКУИ относятся: 1. длина канала 2. мощность 3. ширина спектра	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Как называются опасные сигналы, которые создаются техническим средством обработки информации для выполнения заданных функций? 1. Случайные 2. Намеренные 3. Функциональные	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Как называется сигнал, который передает защищаемую информацию и может быть перехвачен злоумышленником с дальнейшим извлечением этой информации? 1. демаскирующий 2. опасный 3. информационный	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Произведение значений длительности передачи сигнала, его динамического диапазона и диапазона частот называется: 1. длиной сигнала 2. объемом сигнала 3. шириной сигнала	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2	30

		ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
6	Как называется преобразование модулированного сигнала с целью выделения из него информационной составляющей? 1. Дискретизация 2. Демодуляция 3. Декодирование	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Как называется признак защищаемого сигнала, позволяющий обнаруживать и распознавать его среди других сигналов? 1. Информационный 2. Демаскирующий 3. Основной	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Разность между максимальной и минимальной частотой в спектре сигнала называется: 1. динамическим диапазоном 2. статическим диапазоном 3. шириной спектра	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	Как называются преобразователи внешних акустических сигналов в электрические? 1. Стетоскопы 2. Радиозакладки 3. акустоэлектрические преобразователи	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Как называются акустоэлектрические преобразователи, в которых под воздействием акустической волны возникают эквивалентные	ПК 3.1 ПК 3.2	30

	электрические сигналы? 1. Электрические 2. активные 3. пассивные	ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	

3.1.4. Тестовые вопросы для промежуточной аттестации по Теме 1.4. Методы и средства технической разведки

Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	Как называется совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Как называется бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	В каком техническом канале утечки информации носителем является упругая акустическая волна?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Как называется пространство, в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1	30

		ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
5	Как называется технический канал утечки информации, при котором производится съем информации с линии связи контактного подключения аппаратуры злоумышленника?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	Что значит буква "Н" в аббревиатуре ПЭМИН?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	… шпионаж нужен, так как конкуренты тоже заинтересованы в информации о вас и пытаются собрать о вас информацию	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	деятельность по сбору информации о конкурентах, а также деятельность во избежание получения информации конкурентами о нас	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	«сырая» информация, которая прошла первичное распределение,	ПК 3.1	30

	отбор и информационную обработку и сконцентрированная вокруг одного интересующего нас предмета, причем в практическом ее приложении	ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
10	сбор информации об определенных интересующих нас вопросах с целью принятия практических решений по этим вопросам	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	Что должно включать в себя описание технического канала утечки информации? 1. описание приемника, среды передачи и источника информативного сигнала 2. описание приемника и источника информативного сигнала 3. описание среды передачи информативного сигнала 4. описание источника информативного сигнала и среды передачи	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Что является носителем информации в оптическом канале утечки информации? 1. Акустическая волна 2. Электрическое поле 3. Электромагнитное поле	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	В каких технических каналах утечки акустической информации основным средством съема информации является микрофон? 1. Воздушные 2. Вибрационные 3. электроакустические	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2	30

		ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
4	В каких технических каналах утечки акустической информации основным средством съема информации является лазер? 1. Вибрационные 2. Электроакустические 3. оптико-электронные	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Выделите способы получения видовой информации: 1. наблюдение за объектами 2. перехват ПЭМИН 3. перехват излучений на частотах работы ВЧ-генераторов 4. съемка объектов	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	К какому типу технических каналов утечки относится перехват информации путем высокочастотного облучения технических средств? 1. Электромагнитные 2. Параметрические 3. Электрические	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Какой этап является первым в процессе построения модели угроз ИС? 1. Идентификация угроз безопасности информации и их источников 2. Определение актуальных угроз безопасности информации 3. Область применения процесса определения угроз безопасности информации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Как называется основной орган внешней разведки Российской Федерации?	ПК 3.1 ПК 3.2	30

	1. ФСТЭК России 2. ФСБ России 3. СВР России	ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
9	Срок действия лицензии: 1. Бессрочно 2. Не более 5 лет 3. 3 года	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	В течение какого срока после оплаты государственной пошлины соискатель может получить лицензию? 1. 2 дня 2. 3 дня 3. неделя	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

3.1.5. Тестовые вопросы для промежуточной аттестации по Теме 1.5. Физические основы утечки информации

Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	В чем измеряются уровень силы звука и уровень звукового давления?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Что является средой распространения сигнала в виброакустическом канале утечки информации?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1	30

		ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
3	Какое средство используется злоумышленником для снятия информации с оптико-электронного канала утечки?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Как называются технические каналы утечки информации, которые образуются в результате того, что звуковая волна давит на элементы схем, проводов и т.п. в ВТСС и ОТСС, изменяя индуктивность и емкость?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Как называется устройство разведки, которое передает информацию злоумышленнику с помощью электромагнитных волн радиочастотного диапазона?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	По какому каналу передает информацию ИК-передатчик?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Как называются закладки, использующие для передачи информации	ПК 3.1	30

	силовые линии?	ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
8	Что располагается в узлах фазированной акустической решетки плоского микрофона?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	В каком техническом канале утечки информации в качестве носителей выступают электрические, электромагнитные и магнитные поля? 1. Оптический 2. Радиоэлектронный 3. Акустический	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	В каком техническом канале утечки информации в качестве носителей используются фотоны? 1. Оптический 2. Акустический 3. Радиоэлектронный	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	В каком техническом канале утечки информации в качестве носителей используются упругие акустические волны? 1. Оптический 2. Радиоэлектронный 3. Акустический	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2	30

		ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
4	Информативность канала оценивается по: 1. Постоянные 2. Периодические 3. Эпизодические	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Каналы, в которых утечка информации носит достаточно регулярный характер, называются: 1. Постоянные 2. Периодические 3. Эпизодические	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	Как называются параметры сигнала, которые изменяются в зависимости от передаваемой информации? 1. Ценные 2. Несущие 3. Информативные	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Утечка информации – это … 1. несанкционированный процесс переноса информации от источника к злоумышленнику 2. процесс раскрытия секретной информации 3. процесс уничтожения информации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Основные риски информационной безопасности: 1. Искажение, уменьшение объема, перекодировка информации	ПК 3.1 ПК 3.2	30

	2. Техническое вмешательство, выведение из строя оборудования сети 3. Потеря, искажение, утечка информации	ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
9	Утечкой информации в системе называется ситуация, которая характеризуется: 1. Потерей данных в системе 2. Изменением формы информации 3. Изменением содержания информации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Основные функции системы безопасности: 1. Установление регламента, аудит системы, выявление рисков 2. Установка новых офисных приложений, смена хостинг-компании 3. Внедрение аутентификации, проверки контактных данных пользователей	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

3.1.6. Тестовые вопросы для промежуточной аттестации по Теме 1.6. Системы защиты от утечки информации

Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	Сотрудник являющийся источником утечки информации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Преимуществом какого режима является возможность предотвратить утечку информации?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1	30

		ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
3	Верно ли, что невозможность предотвратить утечку информации является главным недостатком режима архива?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Верно ли, что для выявления источников и каналов утечки информации, руководство предприятия внедряет политики внутренней безопасности гласно	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Правда ли, что главный принцип эффективной защиты каналов утечки данных – это контроль копируемой информации "до" того, как она будет скопирована?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	Может ли копирование информации из документа привести к утечке информации?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Является ли невозможность предотвратить утечку информации	ПК 3.1	30

	главным недостатком режима архива?	ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
8	В случае формирования конфиденциальных документов с помощью информации, представленной на неконфиденциальных накопителях информации, неконфиденциальные накопители информации должны быть:	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	Подключение ЛВС к другой автоматизированной системе иного класса защищенности должно осуществляться с помощью:	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Как называется вредоносная программа, распространяющаяся по сетевым каналам, способная к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	В чем состоит главный принцип эффективной защиты каналов утечки данных? 1. контроль копируемой информации "до" того, как она будет скопирована 2. комплексный контроль всех каналов	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2	30

	3. контроль и аудит всех передаваемых данных	ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
2	В чем состоит смысл классификации данных? 1. для понимания, что нужно защищать 2. для создания реестра 3. для выполнения требований законов	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	К какой группе действий, которые могут привести к утечке конфиденциальной информации, относится копирование файла на сменные носители? 1. копирование информации из документа 2. перемещение документа, как единого целого 3. изменение документа с целью обмануть следящие системы	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	В чем состоят главные принципы защиты конфиденциальной информации на уровне хранения физических носителей? 1. анонимизация и шифрование 2. шифрование и постоянный надзор 3. отказ от использования физических носителей	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	В каких случаях не следует афишировать установку системы защиты от внутренних угроз? 1. если основная цель внедрения системы - выявление уже действующего канала утечки, определение всех его звеньев 2. если основная цель внедрения системы - обеспечение сохранности информации 3. если основная цель внедрения системы - обеспечение конкурентного преимущества	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	В каком случае цель проекта защиты конфиденциальной информации предполагает скрытое внедрение технических средств?	ПК 3.1 ПК 3.2	30

	1. защита данных 2. выявление источников и каналов утечки данных 3. соответствие требованиям законов	ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
7	Какой из методов защиты каналов утечки данных наиболее эффективен? 1. контроль выноса с территории компании физических носителей 2. скрытое видеонаблюдение и кадровая работа 3. контроль копируемой информации "до" того, как она будет скопирована	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	К какой группе действий, которые могут привести к утечке конфиденциальной информации, относится копирование информации из документа в буфер Windows? 1. перемещение документа, как единого целого 2. копирование информации из документа 3. изменение документа с целью обмануть следящие системы	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	Как Вы считаете, какие цели преследует руководство предприятия, если оно внедряет политики внутренней безопасности тайно, стараясь замаскировать эту деятельность? 1. выявление источников и каналов утечки информации 2. сохранение информации 3. создание конкурентного преимущества	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	В каких случаях установка программного обеспечения маскируется под обновление другой системы безопасности? 1. для обеспечения сохранности информации 2. для выявления источников и каналов утечки информации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7	30

		ОК 9	

3.1.7. Тестовые вопросы для промежуточной аттестации по Теме 2.1. Цели и задачи физической защиты объектов информатизации

Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	Специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности это:	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Какой орган государственной власти является правопреемником Гостехкомиссии России?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	По результатам проведения комплекса организационно-технических мероприятий, в результате которых подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации выдается:	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Какие меры защиты информации предусматривают использование конструктивных решений и технологических особенностей обработки информации ограниченного доступа на объектах информатизации?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	При необходимости подтверждения соответствия системы активной защиты информации установленным требованиям проводится процедура:	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	Можно ли в качестве активной технической меры выбрать установку	ПК 3.4	30

	сертифицированной антивирусной программы?	ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
7	состояние защищенности от внутренних и внешних угроз, обеспечивающее заданное функционирование объекта, не допуская диверсий, аварий, ситуаций, опасных для людей и окружающей среды	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	установление факта несанкционированного действия	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	Какой орган государственной власти осуществляет аттестацию объектов информатизации по требованиям безопасности?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Как называется совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов, в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	Выберите объект испытаний при проведении процедуры аттестации: 1. Индивидуальный предприниматель 2. Средство контроля эффективности защиты информации 3. Помещение для проведения конфиденциальных переговоров	ПК 3.4 ОК 1 ОК 2 ОК 3	30

		ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
2	Государственная система защиты информации включает в себя: 1. Подсистему сертификации СЗИ и подсистему лицензирования в области ЗИ 2. Подсистему сертификации СЗИ и подсистему аттестации ОИ 3. Подсистему лицензирования в области ЗИ и подсистему аттестации ОИ	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Выберите из ниже предложенного объекты информатизации, подлежащие защите: 1. Автоматизированные системы 2. Средство защиты информации 3. Система размножения документов	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Выберите объект испытаний при проведении процедуры лицензирования: 1. Объект информатизации 2. Средство защиты информации 3. Юридическое лицо	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	К какому типу мер по защите информации относится установка уплотнителей в дверном проеме защищаемого помещения? 1. Организационная 2. Активная техническая 3. Пассивная техническая	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	В какой процедуре участвует третья сторона – испытательная лаборатория? 1. Аттестация 2. Аккредитация 3. Сертификация	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Выберите виды мероприятий по защите информации: 1. Технические пассивные	ПК 3.4 ОК 1	30

	2. Активные 3. Организационные пассивные 4. Технические активные	ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
8	Выберите стороны, участвующие в процессе лицензирования: 1. Юридическое лицо и ФСТЭК России 2. Орган по аттестации и испытательная лаборатория 3. Заявитель и орган по аттестации	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	В соответствии с каким документом производится аттестация объекта информатизации? 1. Положение по аттестации объектов информатизации по требованиям безопасности информации 2. Указ Президента “Об аттестации объектов информатизации по требованиям безопасности информации” 3. ФЗ “Об аттестации”	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Расходы за проведение аттестации объекта информатизации по требованиям безопасности возлагаются на: 1. ФСТЭК 2. Орган по аттестации 3. заказчика	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

3.1.8. Тестовые вопросы для промежуточной аттестации по Теме 2.2. Общие сведения о комплексах инженерно-технических средств физической защиты

Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Как называется попытка реализации угрозы?	ПК 3.4 ОК 1 ОК 2	30

		ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
3	Что такое IDS?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	… средства- включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	… средства- сюда входят приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	… средства- охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	… средства- это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	… канал- предполагает канал воздушной проводимости звуковых	ПК 3.4	30

	колебаний в диапазоне слухового восприятия человека.	ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
9	… канал- связан с распространением колебаний звуковой частоты по строительным конструкциям и инженерным коммуникациям.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	… канал- переносчиком информации выступает свет, испускаемый источником конфиденциальной информации или отраженный от него в видимом, инфракрасном и ультрафиолетовом диапазонах	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	Что является входами системы защиты информации? 1. внешние и внутренние угрозы 2. злоумышленники и владельцы информации 3. средства и методы защиты	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Что является выходами системы защиты информации? 1. внешние и внутренние угрозы 2. злоумышленники и владельцы информации 3. средства и методы защиты	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется: 1. активный перехват; 2. аудиоперехват; 3. видеоперехват;	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4	30

		ОК 5 ОК 6 ОК 7 ОК 9	
4	Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой? 1. Анализ связующего дерева 2. NIST 3. Анализ сбоев и дефектов	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Что представляет собой стандарт ISO/IEC 27799? 1. Стандарт по защите персональных данных о здоровье 2. Новая версия BS 17799 3. Определения для новой серии ISO 27000 4. Новая версия NIST 800-60	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	Что входит в группу физических средств защиты? 1. различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий 2. приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации 3. специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Что входит в группу аппаратных средств защиты? 1. различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий 2. приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации 3. специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Что входит в группу программных средств защиты? 1. различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным	ПК 3.4 ОК 1 ОК 2 ОК 3	30

	носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий 2. приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации 3. специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных	ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
9	Что входит в группу криптографических средств защиты? 1. различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий 2. математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования 3. специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Канал, который предполагает канал воздушной проводимости звуковых колебаний в диапазоне слухового восприятия человека. 1. Акустический 2. Вибро-акустический 3. Визуально-оптический	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

3.1.9. Тестовые вопросы для промежуточной аттестации по Теме 2.3. Система обнаружения комплекса инженерно-технических средств физической защиты

Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	Подсистема … предназначена для обнаружения попыток и/или фактов совершения НСД. Эффективность работы всей СФЗ основывается на надежном (и своевременном) обнаружении НСД.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	совокупность технических средств и мероприятий, нацеленных на предотвращение утечек, разглашения информации, и несанкционированного доступа в сетевые ресурсы организации	ПК 3.4 ОК 1 ОК 2 ОК 3	30

		ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
3	процесс распознавании субъекта (объект А. по присущему или присвоенному ему идентификационному признаку	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	процесс проверки принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Электронный прибор, позволяющий обнаруживать металлические предметы в нейтральной или слабопроводящей среде за счёт их проводимости	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	Маленькие фокусные расстояния (f) в камерах видеонаблюдения характерны для:	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Чувствительность камеры видеонаблюдения измеряется в...	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Для ночной освещенности объектов характерно следующее количество люкс:	ПК 3.4 ОК 1	30

		ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
9	совокупность ячеек, способных передавать информацию о свете	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	устройство для получения информации о состоянии контролируемой им системы, преобразующее данные об изменении характеристик исследуемой области в сигнал, удобный для дальнейшего использования	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	Вид инженерно-технической защиты информации, который используется с целью решения задач по охране предприятия, наблюдению за территорией и помещениями, осуществлению контролируемого доступа в здание. 1. Физический 2. Аппаратный 3. Программный 4. Криптографический	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Вид инженерно-технической защиты информации, к которому относятся электронные и механические устройства, предназначенные для инженерно-технической защиты информации и для противодействия шпионажу. 1. Физический 2. Аппаратный 3. Программный 4. Криптографический	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Вид инженерно-технической защиты информации, который включает в себя системы по защите информации, обеспечивающие защиту секретных данных: проектов, чертежей, стратегических и тактических задач фирмы, финансовых и бухгалтерских данных, сведений о работающих сотрудниках. 1. Физический	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5	30

	2. Аппаратный 3. Программный 4. Криптографический	ОК 6 ОК 7 ОК 9	
4	К какому виду инженерно-технической защиты информации относятся специальные системы шифрования и кодировки, которые используются для защиты информации при телефонных переговорах, рабочих встречах, в рамках совещаний. Принцип работы криптографии состоит в применении математических моделей кодировки сообщений, что обеспечивает эффективную защиту информации от несанкционированного изменения и использования злоумышленниками. 1. Физический 2. Аппаратный 3. Программный 4. Криптографический	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Расшифруйте аббревиатуру СКУД: 1. Система контроля и управления доступом 2. Система катализации и управления доступом 3. Система карт и управления доступом	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	СКУД по среднему количеству емкости точек доступа обычно содержит: 1. от 32 до 64 точек доступа; 2. от 16 до 64 точек доступа; 3. от 50 до 100 точек доступа;	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	СКУД обычно интегрируется… 1. С системой видеонаблюдения и системой охранно-пожарной сигнализации; 2. С системой вентиляцией на предприятии; 3. С системой охранной; 4. С системой пожарной.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Если СКУД идентифицируется по карточке и отпечатку пальца, то он классифицируется как: 1. Многоуровневый; 2. Двухступенчатый. 3. Одноуровневый 4. Одноступенчатый	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	Главным отличием автономных СКУД от сетевых	ПК 3.4	30

	(централизованных) является: 1. Автономные могут функционировать без центрального пульта охраны; 2. Количество точек на предприятии; 3. Сетевой может обходится без блока питания.	ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
10	Что не относится к идентификаторам типа eToken? 1. малые размеры, удобство хранения; 2. отсутствие аппаратного считывателя; 3. простота подсоединения к USB-порту; 4. можно использовать как флэш-накопитель.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

3.1.10. Тестовые вопросы для промежуточной аттестации по Теме 2.4. Система контроля управления доступом

Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	Расшифруйте аббревиатуру СКУД	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Можно ли назвать проходные шлюзы устройством, преграждающим управляемым (УПУ)?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Если СКУД идентифицируется по карточке и отпечатку пальца, то он классифицируется как	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Обеспечение безопасности и охраны объектов не осуществляется подразделениями:	ПК 3.4 ОК 1	30

		ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
5	совокупность создаваемых имеющими право на создание ведомственной охраны федеральными органами исполнительной власти и организациями органов управления, сил и средств, предназначенных для защиты охраняемых объектов от противоправных посягательств	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	государственное полицейское подразделение, осуществляющее охрану особо важных и режимных объектов (в том числе подлежащих обязательной охране войсками национальной гвардии), имущества физических и юридических лиц по договорам;	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Расщифруйте РСП	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Расшифруйте «отдел СП»	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	Расшифруйте «отдел СИ»	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

10	Именно этот протокол объединил отдельные компьютерные сети во всемирную сеть Интернет	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	Расшифруйте аббревиатуру СКУД: 4. Система контроля и управления доступом 5. Система катализации и управления доступом 6. Система карт и управления доступом	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	СКУД по среднему количеству емкости точек доступа обычно содержит: 4. от 32 до 64 точек доступа; 5. от 16 до 64 точек доступа; от 50 до 100 точек доступа;	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	СКУД обычно интегрируется… 5. С системой видеонаблюдения и системой охранно-пожарной сигнализации; 6. С системой вентиляцией на предприятии; 7. С системой охранной; 8. С системой пожарной.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Если СКУД идентифицируется по карточке и отпечатку пальца, то он классифицируется как: 5. Многоуровневый; 6. Двухступенчатый. 7. Одноуровневый Одноступенчатый	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Обеспечение безопасности и охраны объектов не осуществляется подразделениями: 1. государственной, ведомственной, вневедомственной охраны; 2. частными охранными предприятиями;	ПК 3.4 ОК 1 ОК 2 ОК 3	30

	3. нечастными охранными предприятиями.	ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
6	Система охраны предприятия - это... 1. совокупность используемых для охраны предприятия сил и средств, а также способов и методов охраны предприятия и его объектов; 2. система средств, а также способов и методов охраны предприятия и его объектов; 3. система физического и технического контроля объектов защиты от злоумышленников.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Ведомственная охрана - это... 1. совокупность создаваемых имеющими право на создание ведомственной охраны федеральными органами исполнительной власти и организациями органов управления, сил и средств, предназначенных для защиты охраняемых объектов от противоправных посягательств; 2. государственное полицейское подразделение, осуществляющее охрану особо важных и режимных объектов (в том числе подлежащих обязательной охране войсками национальной гвардии), имущества физических и юридических лиц по договорам; 3. организация, специально учрежденная для оказания охранных услуг, зарегистрированная в установленном законом порядке и имеющая лицензию на осуществление частной охранной деятельности.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Вневедомственная охрана это... 1. совокупность создаваемых имеющими право на создание ведомственной охраны федеральными органами исполнительной власти и организациями органов управления, сил и средств, предназначенных для защиты охраняемых объектов от противоправных посягательств; 2. государственное полицейское подразделение, осуществляющее охрану особо важных и режимных объектов (в том числе подлежащих обязательной охране войсками национальной гвардии), имущества физических и юридических лиц по договорам; 3. организация, специально учрежденная для оказания охранных услуг, зарегистрированная в установленном законом порядке и имеющая лицензию на осуществление частной охранной деятельности.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	Подключение к интернету с помощью прокси-сервера может помочь: 1. ускорить работу в интернете 2. скрыть свой IP-адрес 3. заходить на сайты, доступ к которым ограничил системный администратор 4. все ответы верны	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7	30

		ОК 9	
10	Исследовании окружающего пространства с помощью звуковых волн, не распознаваемых для человека характерно для ... 1. ИК датчиков движения; 2. УЗ датчиков движения;	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

3.1.11. Тестовые вопросы для промежуточной аттестации по Теме 2.5. Система телевизионного наблюдения

Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	Назначение какой системы является обеспечение визуального контроля над обстановкой на объекте?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Отвечает ли система безопасности гостиничного комплекса за защиту технической базы компьютера?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Разрешение для аналоговых видеокамер измеряется...	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	программно-аппаратный комплекс (видеокамеры, объективы, мониторы, регистраторы и др. оборудование), предназначенный для организации видеоконтроля как на локальных, так и на территориально-распределённых объектах.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

5	Любая система телевизионного наблюдения включает три функциональные части: телевизионные камеры, аппаратуру обработки видеоинформации и …	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	телевизионная система замкнутого типа, предназначенная для получения телевизионных изображений с охраняемого объекта в целях обеспечения противокриминальной защиты	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	наблюдение, осуществляемое непосредственно (глазами человека) или с помощью дополнительных оптических средств (между глазами человека и наблюдаемым объектом), например бинокля.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	формирование и передача видеосигналов на расстояние	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	ТВ классифицируются на системы: замкнутые, квазизамкнутые и …	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	… телевизионная камера – это телекамера, имеющая встроенный интерфейс для передачи видеоизображения по компьютерной сети.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6	30

		ОК 7 ОК 9	

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	Проверка истинности поступающих сигналов тревоги осуществляется: 1. Системой телевизионного наблюдения 2. Системой визуально звукового оповещения 3. Системой охраны 4. все варианты	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Техническая укрепленность здания гостиницы необходима для 1. препятствия несанкционированному проникновению в здания гостиничного комплекса 2. сейсмоустойчивости 3. продления срока службы здания 4. все варианты	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Разрешение для аналоговых видеокамер измеряется... 1. Телевизионными линиями (ТВЛ) 2. Количеством пикселей 3. СВЧ датчиков движения	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Какая возможность есть у абонентов IP-телевидения в отличие от телезрителей аналогового кабельного ТВ: 1. просмотр передач и фильмов с разными звуковыми дорожками (например, на русском языке или языке оригинала). 2. просмотр передач и фильмов 3D-формате 3. просмотр двух и более каналов одновременно на одном телевизоре	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	телекамера, в которой в цифровой форме происходит как формирование видеоизображения и его предварительная обработка, так и дальнейшая передача по каналам связи (т.е. имеется цифровой интерфейс). 1. Цифровая 2. Аналоговая 3. Сетевая	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	телекамера, имеющую аналоговый интерфейс для подключения к	ПК 3.4	30

	каналу связи. 1. Цифровая 2. Аналоговая 3. Сетевая	ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
7	Телекамера, имеющая встроенный интерфейс для передачи видеоизображения по компьютерной сети 1. Цифровая 2. Аналоговая 3. Сетевая	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Система с формированием видеосигнала аналоговыми телекамерами, обработкой и передачей видеосигналов по каналам связи в аналоговой форме. 1. Аналоговая ТВ-система 2. Цифровая ТВ-система 3. Сетевая ТВ-система 4. ТВ-система высокой четкости	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	Система с формированием видеосигнала цифровыми телекамерами, обработкой и передачей видеосигналов по каналам связи в цифровой форме 1. Аналоговая ТВ-система 2. Цифровая ТВ-система 3. Сетевая ТВ-система 4. ТВ-система высокой четкости	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Система, использующие в качестве каналов связи компьютерные сети и сжатие передаваемого сигнала 1. Аналоговая ТВ-система 2. Цифровая ТВ-система 3. Сетевая ТВ-система 4. ТВ-система высокой четкости	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

3.1.12. Тестовые вопросы для промежуточной аттестации по Теме 2.6. Система сбора, обработки, отображения и документирования информации

Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	совокупность устройств, предназначенных для передачи, приема, сбора, обработки, регистрации и представления оператору	ПК 3.4 ОК 1	30

	информации от средств выявления, а также для дистанционного управления устройствами технических средств охраны, контроля работоспособности извещения и каналов передачи информации	ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
2	область памяти компьютера, предназначенная для хранения электронных сообщений, документов или данных, передаваемых по электронной почте.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Совокупность программ для управления вычислительным процессом персонального компьютера или вычислительной сети — это	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Компьютер, на котором содержатся файлы, предназначенные для открытого доступа, — это	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Информация, преимущественное право на использование которой принадлежит одному лицу или группе лиц, — это	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	экземпляр, который полностью повторят содержание подлинника	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

7	Правильно ли высказывание, приведенное ниже: Одна из задач систем управления документооборотом – распределить общие информационные ресурсы организации:	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	какой-либо материальный носитель с информацией, которая обладает определенными реквизитами;	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	Внутреннее согласование называется	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Вид организационного документа, который определяет порядок образования, структуру и организацию работы предприятия	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	Какой из перечисленных принципов не относится к принципам построения организационных форм обработки данных? 1. принцип толерантности 2. принцип эффективности 3. принцип системности	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	АРМ руководителя: 1. предназначено для выполнения функций оперативного управления и функций принятия решений 2. предоставляет пользователю возможность проводить	ПК 3.4 ОК 1 ОК 2 ОК 3	30

	аналитическую работу, максимально используя всю необходимую информацию 3. позволяет автоматизировать выполняемую пользователем ежедневную рутинную работу	ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
3	Документом является: 1. стандартное расположение материала 2. материальный объект с информацией, зафиксированной созданным человеком способом, для её передачи во времени и пространстве 3. совокупность реквизитов официального письма	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Информация, которая имеет структуру и содержится на носителе: 1. документированная информация 2. делопроизводство 3. официальный документ	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Способность документа повлечь за собой правовые последствия: 1. достоверность 2. юридическая значимость 3. юридическая сила	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	Обязательный элемент оформления документа называется: 1. образцом 2. реквизитом 3. формуляром	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Что заполняют при обработке документов на компьютере: 1. карточку учета документов 2. регистрационную карточку на дисплее, а регистрационный номер ставят на сам документ 3. журнал регистрации и заполняют на документе реквизит отметку о поступлении документа	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Какой реквизит организационно-распорядительного документа является переменным:	ПК 3.4 ОК 1	30

	1. код формы документа 2. наименование организации 3. дата документа	ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
9	Какого вида печати не существует: 1. простой 2. гербовой 3. универсальной	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Способность документа повлечь за собой правовые последствия: 1. достоверность 2. юридическая значимость 3. юридическая сила	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

3.1.13. Тестовые вопросы для промежуточной аттестации по Теме 2.7. Система воздействия

Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	Многофункциональный поисковый прибор … предназначен для проведения мероприятий по обнаружению и локализации специальных технических средств (СТС) негласного получения информации, для выявления естественных и искусственно созданных каналов утечки информации, а также для контроля качества защиты информации	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Нелинейный … NR-900EMS (ЮТДН.468165.008), предназначен для поиска скрытно установленных технических средств съема информации	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Какая часть изделия NR-900EMS изображена на рисунке под номером 4	ПК 3.4 ОК 1 ОК 2	30

		ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
4	Измеритель спектра вторичных полей (детектор нелинейных переходов) “… ” (далее по тексту - изделие) предназначен для поиска электронных устройств, содержащих полупроводниковые компоненты, независимо от их функционального состояния.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	выходной разъем передатчика NR 900 EM, маркированный красной точкой;	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	Изделие NR 900 EM обеспечивает возможность работы в условиях помех от сигналов сотовой связи стандарта 1. GSM-1800 2. GSL-1800 3. GSM-1600	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	На верхней поверхности блока прибора ST 033P Пиранья расположены: 1. графический индикатор 2. встроенный громкоговоритель 3. крышка батарейного отсека	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6	30

		ОК 7 ОК 9	
3	Установка звукового контроля на приборе ST 033P Пиранья производится нажатием на кнопку «…». 1. ENTER 2. START 3. RUN	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Какое устройство изображено на рисунке? 1. ST 033P Пиранья 2. NR 900 EM 	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Какое устройство изображено на рисунке? 1. ST 033P Пиранья 2. NR 900 EM 	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

3.1.14. Тестовые вопросы для промежуточной аттестации по Теме 2.8. Применение инженерно-технических средств физической защиты

Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Как называется попытка реализации угрозы?	ПК 3.4	30

		ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
3	Что такое IDS?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	… средства- включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	… средства- сюда входят приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	… средства- охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	… средства- это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7	30

		ОК 9	
8	… канал- предполагает канал воздушной проводимости звуковых колебаний в диапазоне слухового восприятия человека.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	… канал- связан с распространением колебаний звуковой частоты по строительным конструкциям и инженерным коммуникациям.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	… канал- переносчиком информации выступает свет, испускаемый источником конфиденциальной информации или отраженный от него в видимом, инфракрасном и ультрафиолетовом диапазонах	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	Вид инженерно-технической защиты информации, который используется с целью решения задач по охране предприятия, наблюдению за территорией и помещениями, осуществлению контролируемого доступа в здание. 5. Физический 6. Аппаратный 7. Программный Криптографический	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Вид инженерно-технической защиты информации, к которому относятся электронные и механические устройства, предназначенные для инженерно-технической защиты информации и для противодействия шпионажу. 5. Физический 6. Аппаратный 7. Программный Криптографический	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Вид инженерно-технической защиты информации, который включает в себя системы по защите информации, обеспечивающие защиту секретных данных: проектов, чертежей, стратегических и	ПК 3.4 ОК 1 ОК 2	30

	тактических задач фирмы, финансовых и бухгалтерских данных, сведений о работающих сотрудниках. 5. Физический 6. Аппаратный 7. Программный Криптографический	ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
4	К какому виду инженерно-технической защиты информации относятся специальные системы шифрования и кодировки, которые используются для защиты информации при телефонных переговорах, рабочих встречах, в рамках совещаний. Принцип работы криптографии состоит в применении математических моделей кодировки сообщений, что обеспечивает эффективную защиту информации от несанкционированного изменения и использования злоумышленниками. 5. Физический 6. Аппаратный 7. Программный Криптографический	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Расшифруйте аббревиатуру СКУД: 7. Система контроля и управления доступом 8. Система катализации и управления доступом 9. Система карт и управления доступом	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	СКУД по среднему количеству емкости точек доступа обычно содержит: 6. от 32 до 64 точек доступа; 7. от 16 до 64 точек доступа; от 50 до 100 точек доступа;	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	СКУД обычно интегрируется… 9. С системой видеонаблюдения и системой охранно-пожарной сигнализации; 10. С системой вентиляцией на предприятии; 11. С системой охранной; 12. С системой пожарной.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Если СКУД идентифицируется по карточке и отпечатку пальца, то он классифицируется как: 8. Многоуровневый; 9. Двухступенчатый. 10. Одноуровневый Одноступенчатый	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6	30

		ОК 7 ОК 9	
9	Главным отличием автономных СКУД от сетевых (централизованных) является: 4. Автономные могут функционировать без центрального пульта охраны; 5. Количество точек на предприятии; Сетевой может обходится без блока питания.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Что не относится к идентификаторам типа eToken? 5. малые размеры, удобство хранения; 6. отсутствие аппаратного считывателя; 7. простота подсоединения к USB-порту; можно использовать как флэш-накопитель.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

3.1.15. Тестовые вопросы для промежуточной аттестации по Теме 2.9. Эксплуатация инженерно-технических средств защиты

Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	Подсистема … предназначена для обнаружения попыток и/или фактов совершения НСД. Эффективность работы всей СФЗ основывается на надежном (и своевременном) обнаружении НСД.	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	совокупность технических средств и мероприятий, нацеленных на предотвращение утечек, разглашения информации, и несанкционированного доступа в сетевые ресурсы организации	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	процесс распознавании субъекта (объект А. по присущему или присвоенному ему идентификационному признаку	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7	30

		ОК 9	
4	процесс проверки принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Электронный прибор, позволяющий обнаруживать металлические предметы в нейтральной или слабопроводящей среде за счёт их проводимости	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	Маленькие фокусные расстояния (f) в камерах видеонаблюдения характерны для:	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Чувствительность камеры видеонаблюдения измеряется в...	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Для ночной освещенности объектов характерно следующее количество люкс:	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	совокупность ячеек, способных передавать информацию о свете	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5	30

		ОК 6 ОК 7 ОК 9	
10	устройство для получения информации о состоянии контролируемой им системы, преобразующее данные об изменении характеристик исследуемой области в сигнал, удобный для дальнейшего использования	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	Что является входами системы защиты информации? 1. внешние и внутренние угрозы 2. злоумышленники и владельцы информации 3. средства и методы защиты	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Что является выходами системы защиты информации? 1. внешние и внутренние угрозы 2. злоумышленники и владельцы информации 3. средства и методы защиты	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется: 1. активный перехват; 2. аудиоперехват; 3. видеоперехват;	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой? 1. Анализ связующего дерева 2. NIST 3. Анализ сбоев и дефектов	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Что представляет собой стандарт ISO/IEC 27799?	ПК 3.4	30

	1. Стандарт по защите персональных данных о здоровье 2. Новая версия BS 17799 3. Определения для новой серии ISO 27000 4. Новая версия NIST 800-60	ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
6	Что входит в группу физических средств защиты? 1. различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий 2. приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации 3. специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Что входит в группу аппаратных средств защиты? 1. различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий 2. приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации 3. специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Что входит в группу программных средств защиты? 1. различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий 2. приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты информации 3. специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	Что входит в группу криптографических средств защиты? 1. различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4	30

	осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий 2. математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования 3. специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных	ОК 5 ОК 6 ОК 7 ОК 9	
10	Канал, который предполагает канал воздушной проводимости звуковых колебаний в диапазоне слухового восприятия человека. 1. Акустический 2. Вибро-акустический 3. Визуально-оптический	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

3.1.16. Тестовые вопросы для промежуточной аттестации МДК 03.01
Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	Как называется совокупность информационных ресурсов, средств и систем информатизации, используемых в соответствии с заданной информационной технологией, и систем связи вместе с помещениями (транспортными средствами), в которых они установлены?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Как называется информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Как называется совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3	30

		ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
4	В каком техническом канале утечки информации в качестве носителей выступают электрические, электромагнитные и магнитные поля?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	В каком техническом канале утечки информации в качестве носителей используются фотоны?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	Как называется бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Как называется совокупность условий и факторов, создающих потенциальную угрозу или реально существующую опасность нарушения безопасности информации?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Как называется попытка реализации угрозы?	ПК 3.1 ПК 3.2 ПК 3.3	30

		ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
9	Непосредственная причина возникновения угрозы называется:	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Если злоумышленник внедрил в компьютер вредоносную программу и получил доступ к личной информации пользователя, какое свойство информации было нарушено?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
11	Как называется состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
12	В каком техническом канале утечки информации в качестве носителей используются упругие акустические волны?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

13	Каналы, в которых утечка информации носит достаточно регулярный характер, называются:	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
14	Как называется совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
15	Какая организация курирует Банк данных угроз безопасности информации?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
16	Как называются технические средства защиты, которые ослабляют уровень информативного сигнала?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
17	Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств это…	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5	30

		ОК 6 ОК 7 ОК 9	
18	Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым они были доверены по службе или стали известны в процессе работы, называется ...	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
19	Если в результате DDOS-атаки новостной сайт на какое-то время вышел из строя и был недоступен для пользователей, какое свойство информации было нарушено?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
20	Как называются методы защиты акустической информации, направленные на ослабление непосредственных акустических сигналов, циркулирующих в помещении?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
21	Какой орган государственной власти осуществляет аттестацию объектов информатизации по требованиям безопасности?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
22	Как называются акустоэлектрические преобразователи, в которых под воздействием акустической волны возникают эквивалентные электрические сигналы?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2	30

		ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
23	Какой участник системы аттестации аттестует объекты информатизации по требованиям безопасности и выдает "Аттестаты соответствия"?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
24	Как называются параметры сигнала, которые изменяются в зависимости от передаваемой информации?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
25	Как называется сигнал, который можно представить непрерывной функцией непрерывного аргумента?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
26	Что такое φ в формуле $s(t) = Asin(2\pi ft + \varphi)$?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
27	Сколько уровней амплитуды имеет бинарный сигнал?	ПК 3.1 ПК 3.2	30

		ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
28	Как называется слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
29	Как называется пространство, в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
30	Как называется деятельность по разработке (ведению), утверждению, изменению (актуализации), отмене, опубликованию и применению документов по стандартизации и иная деятельность, направленная на достижение упорядоченности в отношении объектов стандартизации?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
31	Как называется технический канал утечки информации, при котором производится съем информации с линии связи контактного подключения аппаратуры злоумышленника?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7	30

		ОК 9	
32	Как называется технический канал утечки информации, при котором производится съем информации с линии связи контактного подключения аппаратуры злоумышленника?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
33	Что значит буква "Н" в аббревиатуре ПЭМИН?	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
34	… шпионаж нужен, так как конкуренты тоже заинтересованы в информации о вас и пытаются собрать о вас информацию	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
35	деятельность по сбору информации о конкурентах, а также деятельность во избежание получения информации конкурентами о нас	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
36	«сырая» информация, которая прошла первичное распределение, отбор и информационную обработку и сконцентрированная вокруг одного интересующего нас предмета, причем в практическом ее приложении	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4	30

		ОК 5 ОК 6 ОК 7 ОК 9	
37	сбор информации об определенных интересующих нас вопросах с целью принятия практических решений по этим вопросам	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	Что должно включать в себя описание технического канала утечки информации? 1. описание приемника, среды передачи и источника информативного сигнала 2. описание приемника и источника информативного сигнала 3. описание среды передачи информативного сигнала 4. описание источника информативного сигнала и среды передачи	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Что является носителем информации в оптическом канале утечки информации? 1. Акустическая волна 2. Электрическое поле 3. Электромагнитное поле	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	В каких технических каналах утечки акустической информации основным средством съема информации является микрофон? 1. Воздушные 2. Вибрационные 3. электроакустические	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

4	В каких технических каналах утечки акустической информации основным средством съема информации является лазер? 1. Вибрационные 2. Электроакустические 3. оптико-электронные	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	В течение какого срока после оплаты государственной пошлины соискатель может получить лицензию? 1. 2 дня 2. 3 дня 3. неделя	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	Пропускная способность составного канала определяется как: 1. разность наибольшей и наименьшей пропускной способности входящих каналов 2. сумма наибольшей и наименьшей пропускной способности входящих каналов 3. наименьшая пропускная способность входящих каналов	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	К основным показателям ТКУИ относятся: 1. длина канала 2. мощность 3. ширина спектра	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	К какому типу технических каналов утечки относится перехват информации путем высокочастотного облучения технических средств? 1. Электромагнитные 2. Параметрические 3. Электрические	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5	30

		ОК 6 ОК 7 ОК 9	
9	Как называются опасные сигналы, которые создаются техническим средством обработки информации для выполнения заданных функций? 1. Случайные 2. Намеренные 3. Функциональные	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	Срок действия лицензии: 1. Бессрочно 2. Не более 5 лет 3. 3 года	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
11	Как называется сигнал, который передает защищаемую информацию и может быть перехвачен злоумышленником с дальнейшим извлечением этой информации? 1. демаскирующий 2. опасный 3. информационный	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
12	Произведение значений длительности передачи сигнала, его динамического диапазона и диапазона частот называется: 1. длиной сигнала 2. объемом сигнала 3. шириной сигнала	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
13	Как называется преобразование модулированного сигнала с целью выделения из него информационной составляющей? 1. Дискретизация 2. Демодуляция 3. Декодирование	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2	30

		ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
14	Как называется признак защищаемого сигнала, позволяющий обнаруживать и распознавать его среди других сигналов? 1. Информационный 2. Демаскирующий 3. Основной	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
15	Разность между максимальной и минимальной частотой в спектре сигнала называется: 1. динамическим диапазоном 2. статическим диапазоном 3. шириной спектра	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
16	Как называются преобразователи внешних акустических сигналов в электрические? 1. Стетоскопы 2. Радиозакладки 3. акустоэлектрические преобразователи	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
17	Как называются акустоэлектрические преобразователи, в которых под воздействием акустической волны возникают эквивалентные электрические сигналы? 1. Электрические 2. Активные 3. пассивные	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
18	В соответствии с каким документом осуществляется отнесение информации к государственной тайне?	ПК 3.1 ПК 3.2	30

	1. ФЗ “Об информации, информационных технологиях и о защите информации” 2. ФЗ “О техническом регулировании” 3. ФЗ “О государственной тайне”	ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
19	Если автор статьи опубликовал ее в Интернете на сайте со свободным доступом, информацию из этой статьи можно отнести к: 1. конфиденциальной информации 2. государственной тайне 3. общедоступной информации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
20	На кого возлагается ответственность за организацию работ по ТКЗИ в организации? 1. Отдел кадров 2. руководителя подразделения по защите информации 3. руководитель организации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
21	Как называется комплекс административных и ограничительных мер, направленных на защиту информации путем регламентации деятельности персонала и порядка функционирования средств (систем)? 1. правовые меры защиты 2. организационные меры защиты 3. криптографические меры защиты	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
22	Выделите организационные меры защиты информации от утечки по ТКУИ 1. определение границ контролируемой зоны 2. экранирование ОТСС 3. пространственное зашумление	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7	30

		ОК 9	
23	В соответствии с ФЗ №149 "Об информации, информационных технологиях и о защите информации" информация разделяется на следующие категории: 1. общедоступная и конфиденциальная 2. общедоступная и ограниченного доступа 3. ограниченного доступа и государственная тайна	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
24	Какой документ является основным нормативным документом в области регулирования в Российской Федерации? 1. Федеральный закон N 184 "О техническом регулировании" 2. Федеральный закон N 149 "Об информации, информационных технологиях и о защите информации" 3. Федеральный закон N 162 "О стандартизации в Российской Федерации"	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
25	Кто осуществляет формирование требований к системе защиты информации конкретного объекта информатизации? 1. ФСБ 2. ФСТЭК 3. обладатель информации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
26	При входе в домен Windows пароль от учетной записи является… 1. средством идентификации 2. средством аутентификации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
27	Как называется совокупность правил выполнения работ по сертификации, ее участников и правил функционирования системы сертификации в целом? 1. система сертификации 2. система аккредитации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4	30

		ОК 5 ОК 6 ОК 7 ОК 9	
28	В случае формирования конфиденциальных документов с помощью информации, представленной на неконфиденциальных накопителях информации, неконфиденциальные накопители информации должны быть: 1. учтены в специальных журналах 2. отформатированы после обработки 3. открыты на запись 4. закрыты на запись	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
29	Какой участник системы сертификации принимает решение о проведении повторной сертификации при изменениях в технологии изготовления и конструкции (составе) сертифицированных средств защиты информации: 1. федеральный орган по сертификации 2. центральный орган системы сертификации 3. орган по сертификации средств защиты информации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
30	Нормативные правовые акты, затрагивающие права, свободы и обязанности человека относятся к: 4. конфиденциальной информации 1. государственной тайне 2. общедоступной информации	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
31	Какой вид атаки направлен на получение конфиденциальной информации путем прослушивания сети? 1. анализ сетевого трафика 2. сканирование сети 3. навязывание ложного маршрута	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
32	Как называется сигнал, который можно представить непрерывной функцией непрерывного аргумента? 1. Аналоговый 2. Дискретный	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1	30

	3. Импульсный	ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
33	Подключение ЛВС к другой автоматизированной системе иного класса защищенности должно осуществляться с помощью: 1. Коммутатора 2. межсетевого экрана 3. маршрутизатора	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
34	Как называются закладки, использующие для передачи информации силовые линии? 4. ИК-передатчики 5. сетевые закладки 1. радиозакладки	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
35	Как называется признак защищаемого сигнала, позволяющий обнаруживать и распознавать его среди других сигналов? 1. Информационный 2. Основной 3. Демаскирующий	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
36	Установка аппаратного межсетевого экрана относится к: 1. организационным мерам обеспечения безопасности 2. техническим мерам обеспечения безопасности 3. физическим мерам обеспечения безопасности	ПК 3.1 ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
37	К основным показателям ТКУИ относятся:	ПК 3.1	30

	1. длина канала 2. мощность 3. относительная информативность	ПК 3.2 ПК 3.3 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	

3.1.17. Тестовые вопросы для промежуточной аттестации МДК 03.02
Часть 1.

№	Вопрос	ОК/ПК	Время, сек
1	В чем измеряются уровень силы звука и уровень звукового давления?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Что является средой распространения сигнала в виброакустическом канале утечки информации?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Какое средство используется злоумышленником для снятия информации с оптико-электронного канала утечки?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
4	Как называются технические каналы утечки информации, которые образуются в результате того, что звуковая волна давит на элементы схем, проводов и т.п. в ВТСС и ОТСС, изменяя индуктивность и емкость?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	Как называется устройство разведки, которое передает информацию	ПК 3.4	30

	злоумышленнику с помощью электромагнитных волн радиочастотного диапазона?	ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
6	По какому каналу передает информацию ИК-передатчик?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Как называются закладки, использующие для передачи информации силовые линии?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Что располагается в узлах фазированной акустической решетки плоского микрофона?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	Пусть три акустические волны попадают на плоский микрофон, ϕ - угол падения волны по отношению к осевому направлению: $\phi_1 = 30^o, \phi_1 = 60^o, \phi_1 = 0$ (соответственно, для первой, второй и третьей волн). Какая из этих волн ослабнет больше всего?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
10	По какому каналу принимает информацию лазерный микрофон?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7	30

		ОК 9	
11	сотрудник являющийся источником утечки информации	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
12	Преимуществом какого режима является возможность предотвратить утечку информации?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
13	Верно ли, что невозможность предотвратить утечку информации является главным недостатком режима архива?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
14	Верно ли, что для выявления источников и каналов утечки информации, руководство предприятия внедряет политики внутренней безопасности гласно	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
15	Правда ли, что главный принцип эффективной защиты каналов утечки данных – это контроль копируемой информации "до" того, как она будет скопирована?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
16	Может ли копирование информации из документа привести к утечке информации?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5	30

		ОК 6 ОК 7 ОК 9	
17	Является ли невозможность предотвратить утечку информации главным недостатком режима архива?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
18	В случае формирования конфиденциальных документов с помощью информации, представленной на неконфиденциальных накопителях информации, неконфиденциальные накопители информации должны быть:	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
19	Подключение ЛВС к другой автоматизированной системе иного класса защищенности должно осуществляться с помощью:	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
20	Как называется вредоносная программа, распространяющаяся по сетевым каналам, способная к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
21	Специальное разрешение на право осуществления юридическим лицом или индивидуальным предпринимателем конкретного вида деятельности это:	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
22	Какой орган государственной власти является правопреемником Гостехкомиссии России?	ПК 3.4 ОК 1 ОК 2 ОК 3	30

		ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
23	По результатам проведения комплекса организационно-технических мероприятий, в результате которых подтверждается, что объект информатизации соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации выдается:	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
24	Какие меры защиты информации предусматривают использование конструктивных решений и технологических особенностей обработки информации ограниченного доступа на объектах информатизации?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
25	При необходимости подтверждения соответствия системы активной защиты информации установленным требованиям проводится процедура:	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
26	Можно ли в качестве активной технической меры выбрать установку сертифицированной антивирусной программы?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
27	состояние защищенности от внутренних и внешних угроз, обеспечивающее заданное функционирование объекта, не допуская диверсий, аварий, ситуаций, опасных для людей и окружающей среды	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
28	установление факта несанкционированного действия	ПК 3.4 ОК 1	30

		ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
29	Какой орган государственной власти осуществляет аттестацию объектов информатизации по требованиям безопасности?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
30	Как называется совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения объекта информатизации, помещений или объектов, в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров?	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

Часть 2.

№	Вопрос	ОК/ПК	Время, сек
1	Выберите объект испытаний при проведении процедуры аттестации: 1. Индивидуальный предприниматель 2. Средство контроля эффективности защиты информации 3. Помещение для проведения конфиденциальных переговоров	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
2	Государственная система защиты информации включает в себя: 1. Подсистему сертификации СЗИ и подсистему лицензирования в области ЗИ 2. Подсистему сертификации СЗИ и подсистему аттестации ОИ 3. Подсистему лицензирования в области ЗИ и подсистему аттестации ОИ	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
3	Выберите из ниже предложенного объекты информатизации, подлежащие защите: 1. Автоматизированные системы 2. Средство защиты информации 3. Система размножения документов	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5	30

		ОК 6 ОК 7 ОК 9	
4	Выберите объект испытаний при проведении процедуры лицензирования: 1. Объект информатизации 2. Средство защиты информации 3. Юридическое лицо	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
5	К какому типу мер по защите информации относится установка уплотнителей в дверном проеме защищаемого помещения? 1. Организационная 2. Активная техническая 3. Пассивная техническая	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
6	В какой процедуре участвует третья сторона – испытательная лаборатория? 1. Аттестация 2. Аккредитация 3. Сертификация	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
7	Выберите виды мероприятий по защите информации: 1. Технические пассивные 2. Активные 3. Организационные пассивные 4. Технические активные	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
8	Выберите стороны, участвующие в процессе лицензирования: 1. Юридическое лицо и ФСТЭК России 2. Орган по аттестации и испытательная лаборатория 3. Заявитель и орган по аттестации	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
9	В соответствии с каким документом производится аттестация объекта информатизации? 1. Положение по аттестации объектов информатизации по требованиям безопасности информации	ПК 3.4 ОК 1 ОК 2 ОК 3	30

	2. Указ Президента “Об аттестации объектов информатизации по требованиям безопасности информации” 3. ФЗ “Об аттестации”	ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
10	Расходы за проведение аттестации объекта информатизации по требованиям безопасности возлагаются на: 1. ФСТЭК 2. Орган по аттестации 3. заказчика	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
11	В чем состоит главный принцип эффективной защиты каналов утечки данных? 1. контроль копируемой информации "до" того, как она будет скопирована 2. комплексный контроль всех каналов 3. контроль и аудит всех передаваемых данных	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
12	В чем состоит смысл классификации данных? 1. для понимания, что нужно защищать 2. для создания реестра 3. для выполнения требований законов	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
13	К какой группе действий, которые могут привести к утечке конфиденциальной информации, относится копирование файла на сменные носители? 1. копирование информации из документа 2. перемещение документа, как единого целого 3. изменение документа с целью обмануть следящие системы	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
14	В чем состоят главные принципы защиты конфиденциальной информации на уровне хранения физических носителей? 1. анонимизация и шифрование 2. шифрование и постоянный надзор 3. отказ от использования физических носителей	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
15	В каких случаях не следует афишировать установку системы защиты от внутренних угроз?	ПК 3.4 ОК 1	30

	1. сли основная цель внедрения системы - выявление уже действующего канала утечки, определение всех его звеньев 2. если основная цель внедрения системы - обеспечение сохранности информации 3. если основная цель внедрения системы - обеспечение конкурентного преимущества	ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	
16	В каком случае цель проекта защиты конфиденциальной информации предполагает скрытое внедрение технических средств? 1. защита данных 2. выявление источников и каналов утечки данных 3. соответствие требованиям законов	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
17	Какой из методов защиты каналов утечки данных наиболее эффективен? 1. контроль выноса с территории компании физических носителей 2. скрытое видеонаблюдение и кадровая работа 3. контроль копируемой информации "до" того, как она будет скопирована	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
18	К какой группе действий, которые могут привести к утечке конфиденциальной информации, относится копирование информации из документа в буфер Windows? 1. перемещение документа, как единого целого 2. копирование информации из документа 3. изменение документа с целью обмануть следящие системы	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
19	Как Вы считаете, какие цели преследует руководство предприятия, если оно внедряет политики внутренней безопасности тайно, стараясь замаскировать эту деятельность? 1. выявление источников и каналов утечки информации 2. сохранение информации 3. создание конкурентного преимущества	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
20	В каких случаях установка программного обеспечения маскируется под обновление другой системы безопасности? 1. для обеспечения сохранности информации 2. для выявления источников и каналов утечки информации	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

21	В каком техническом канале утечки информации в качестве носителей выступают электрические, электромагнитные и магнитные поля? 1. Оптический 2. Радиоэлектронный 3. Акустический	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
22	В каком техническом канале утечки информации в качестве носителей используются фотоны? 1. Оптический 2. Акустический 3. Радиоэлектронный	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
23	В каком техническом канале утечки информации в качестве носителей используются упругие акустические волны? 1. Оптический 2. Радиоэлектронный 3. Акустический	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
24	Информативность канала оценивается по: 1. Постоянные 2. Периодические 3. Эпизодические	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
25	Каналы, в которых утечка информации носит достаточно регулярный характер, называются: 1. Постоянные 2. Периодические 3. Эпизодические	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
26	Как называются параметры сигнала, которые изменяются в зависимости от передаваемой информации? 1. Ценные 2. Несущие 3. Информативные	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6	30

		ОК 7 ОК 9	
27	Утечка информации – это … 1. несанкционированный процесс переноса информации от источника к злоумышленнику 2. процесс раскрытия секретной информации 3. процесс уничтожения информации	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
28	Основные риски информационной безопасности: 1. Искажение, уменьшение объема, перекодировка информации 2. Техническое вмешательство, выведение из строя оборудования сети 3. Потеря, искажение, утечка информации	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
29	Утечкой информации в системе называется ситуация, которая характеризуется: 1. Потерей данных в системе 2. Изменением формы информации 3. Изменением содержания информации	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30
30	Основные функции системы безопасности: 1. Установление регламента, аудит системы, выявление рисков 2. Установка новых офисных приложений, смена хостинг-компании 3. Внедрение аутентификации, проверки контактных данных пользователей	ПК 3.4 ОК 1 ОК 2 ОК 3 ОК 4 ОК 5 ОК 6 ОК 7 ОК 9	30

3.2. Критерии оценок по типам (видам) заданий

№	Тип (вид) задания	Критерии оценки
1	Устные ответы, письменные развернутые ответы	**Оценка «5»** ставится в том случае, если обучающийся правильно понимает сущность вопроса, дает точное определение и истолкование основных понятий; правильно анализирует условие задачи (вопроса), ответ логичен, умеет выстроить алгоритм поиска ответа самостоятельно; строит ответ по собственному плану, сопровождает ответ новыми примерами, умеет применить знания в новой ситуации; может установить связь между изучаемым и ранееизученным материалом из курса дисциплины, а также с материалом, усвоенным при изучении других дисциплин/модулей.

		Оценка «4» ставится, если ответ обучающегося удовлетворяет основным требованиям к ответу на оценку 5, но дан без использования собственного плана, новых примеров, без применения знаний в новой ситуации, без использования связей с ранее изученным материалом и материалом, усвоенным при изучении других дисциплин/модулей; обучающийся допустил одну ошибку или не более двух недочетов и может их исправить самостоятельно или с небольшой помощью преподавателя. **Оценка «3»** ставится, если обучающийся правильно понимает сущность вопроса, но в ответе имеются отдельные пробелы в усвоении вопросов курса дисциплины, не препятствующие дальнейшему усвоению программного материала; умеет применять полученные знания при решении простых задач (заданий, вопросов) по готовому алгоритму; допустил не более одной грубой ошибкии двух недочетов, не более одной грубой и одной негрубой ошибки, не более двух-трех негрубых ошибок, одной негрубой ошибки и трех недочетов; допустил четыре-пять недочетов. **Оценка «2»** ставится, если обучающийся не овладел основнымизнаниями и умениями в соответствии с требованиями программы и допустил больше ошибок и недочетов, чем необходимо для оценки.
2	Тесты	**«5»** - 100 – 91% правильных ответов **«4»** - 90 - 70% правильных ответов **«3»** - 69 – 52% правильных ответов **«2»** - 51% и менее правильных ответов
3	Доклады, рефераты, эссе, творческие работы	**Оценка «5»** ставится, если выполнены все требования к написанию и защите работы: обозначена проблема и обоснована её актуальность, сделан краткий анализ различных точек зрения на рассматриваемую проблему и логично изложена собственная позиция, сформулированы выводы, тема раскрыта полностью, выдержан объём, соблюдены требования к внешнему оформлению, даны правильные ответы на дополнительные вопросы. **Оценка «4»** основные требования к работе и её защите выполнены, но при этом допущены недочёты. В частности, имеются неточности в изложении материала; отсутствует логическая последовательность в суждениях; не выдержан объём; имеются упущения в оформлении; на дополнительные вопросы при защите даны неполные ответы. **Оценка «3»** имеются существенные отступления от требований к работе. В частности, тема освещена лишь частично; допущены фактические ошибки в содержании или при ответе на дополнительные вопросы; во время защиты отсутствует вывод. **Оценка «2»** тема не раскрыта, обнаруживается существенное непонимание проблемы.

4	Практические задания	**Оценка «5»** выставляется, если обучающийся активно работает в течение всего практического занятия, дает полные ответы на вопросы преподавателя в соответствии с планом практического занятия и показывает при этом глубокое овладение лекционным материалом, способен выразить собственное отношение по данной проблеме, проявляет умение самостоятельно и аргументированно излагать материал, анализировать явления и факты со ссылками на соответствующие источники, делать самостоятельные обобщения и выводы, заключения, рекомендации, правильно выполняет все этапы практического задания. **Оценка «4»** выставляется при условии соблюдения следующих требований: обучающийся активно работает в течение практического занятия, вопросы освещены полно, изложения материала логическое, обоснованное фактами, со ссылками на соответствующие источники, освещение вопросов завершено выводами, обучающийся обнаружил умение анализировать факты и события, а также выполнять учебные задания. Но в ответах допущены неточности, некоторые незначительные ошибки, имеет место недостаточная аргументированность при изложении материала, недостаточно четко сделаны обобщение и выводы. **Оценка «3»** выставляется в том случае, когда обучающийся в целом овладел сути вопросов по данной теме, обнаруживает знание лекционного материала и учебной литературы, пытается анализировать факты и события, делать выводы и решать задачи. Но на занятии ведет себя пассивно, отвечает только по вызову преподавателя, дает неполные ответы на вопросы, допускает грубые ошибки при освещении теоретического материала, не может обобщить и сделать четкие логические выводы. **Оценка «2»** выставляется в случае, когда обучающийся обнаружил несостоятельность осветить вопросы или вопросы освещены неправильно, бессистемно, с грубыми ошибками, отсутствуют понимания основной сути вопросов, выводы, обобщения, обнаружено неумение решать учебные задачи.
5	Лабораторные работы	**Оценка «5»** ставится, если студент демонстрирует знание теоретического и практического материала по теме лабораторной работы, определяет взаимосвязи между показателями условий, даёт правильный алгоритм решения, определяет междисциплинарные связи по условию задания. **Оценка «4»** ставится, если студент демонстрирует знание теоретического и практического материала по теме лабораторной работы, допуская незначительные неточности при решении задания, имея неполное понимание междисциплинарных связей при правильном выборе алгоритма решения задания. **Оценка «3»** ставится, если студент затрудняется с правильной оценкой предложенной задачи, дает неполный ответ, требующий наводящих вопросов преподавателя, выбор алгоритма решения задачи возможен при наводящих вопросах преподавателя. **Оценка «2»** ставится, если студент дает неверную оценку ситуации, неправильно выбирает алгоритм действий.
6	Самостоятельная работа	**Оценка «5»** ставится, если обучающийся демонстрирует знание изученного материала по теме самостоятельной работы, определяет взаимосвязи между показателями задачи, даёт правильный алгоритм решения, определяет междисциплинарные связи по условию задания. **Оценка «4»** ставится, если обучающийся демонстрирует знание изученного материала по теме самостоятельной работы, допуская незначительные неточности при решении задач, имея неполное понимание междисциплинарных

		связей при правильном выборе алгоритма решения задания. **Оценка «3»** ставится, если обучающийся затрудняется с правильным решением предложенного задания, дает неполный ответ, требующий наводящих вопросов преподавателя, выбор алгоритма решения задания возможен при наводящих вопросах преподавателя. **Оценка «2»** ставится, если обучающийся не выполнил предложенное задание.

3.3. Фонд оценочных средств для промежуточной аттестации по ПМ 03 Защита информации в информационно телекоммуникационных системах и сетях с использованием технических средств защиты

I. ПАСПОРТ

Назначение:

Фонд оценочных средств предназначен для контроля и оценки результатов освоения ПМ. 03 по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

II. ЗАДАНИЕ ДЛЯ ЭКЗАМЕНУЮЩЕГОСЯ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М. А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)
Санкт-Петербургский колледж телекоммуникаций им. Э.Т. Кренкеля

Рассмотрено на заседании предметной (цикловой) комиссии _____2022г. Председатель _____Н.В. Кривоносова	***Экзаменационный билет* № Н** По профессиональному модулю ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты Специальность 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем	УТВЕРЖДАЮ Заместитель директора по учебной работе колледжа _____Н.В. Калинина 2022г.

Инструкция для обучающихся

Внимательно прочитайте задание.

Время выполнения задания – 120 минут

Задание 1. Провести оценку защищенности выделенного помещения от утечки информации по электромагнитному каналу на основании исходных данных (Приложение 1)

Задание 2. Провести оценку защищенности выделенного помещения от утечки информации по акустическому каналу на основании исходных данных (Приложение 2)

*Преподаватель*_____И.О. Фамилия

III. ПАКЕТ ЭКЗАМЕНАТОРА

III а. УСЛОВИЯ

Время выполнения задания – 120 минут

Оборудование:

- посадочные места с ПК по количеству обучающихся;
- рабочее место преподавателя;
- калькуляторы.

Работа обучающегося оценивается путем устного ответа с демонстрацией и пояснением выполненной работы. Длительность ответа – не более 10 минут.

III б. КРИТЕРИИ ОЦЕНКИ

Критерии оценки ответа, экзаменующегося:

оценка «5»	– полностью раскрыто содержание материала в объеме, предусмотренном программой; – изложен материал грамотным языком в определенной логической последовательности, точно используя специализированную терминологию и символику; – правильно выполнено графическое изображение, схему, модель, программу сопутствующие ответу
оценка «4»	– ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков: – в изложении допущены небольшие пробелы, не исказившие логического и информационного содержания ответа; – допущены ошибка или более двух недочетов в графическом представлении материала.
оценка «3»	– неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения программного материала, – имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, моделях, блок-схем, графиков.
оценка «2»	– не раскрыто основное содержание материала; – обнаружено незнание или непонимание обучающимся большей или наиболее важной части учебного материала, – допущены ошибки в определении понятий, при использовании терминологии, в моделях, – блок-схем, графиков

Дополнительно членами комиссии при оценивании обучающегося учитываются:

Показатели оценки результата	**Оценка (да / нет)**
Грамотность речи при устном обосновании материала	
Аргументированность изложения материала	
Соблюдение регламента ответов	
Способность проявлять ответственность за результат выполнения задания	
Грамотность использования ИКТ при выборе материала	
Соблюдение профессиональной этики при ответе	

4. ЛИСТ СОГЛАСОВАНИЯ

Дополнения и изменения к комплекту КОС

Дополнения и изменения к комплекту КОС на_____учебный год по профессиональному модулю _____

В комплект КОС внесены следующие изменения:

_____

_____

_____

_____

_____

Дополнения и изменения в комплекте КОС обсуждены на заседании предметной цикловой комиссии информационной безопасности телекоммуникационных систем

«____»_____20_____г. (протокол №_____).

Председатель ЦК _____ Н.В. Кривоносова

Приложение 1

Оценка защищенности выделенного помещения от утечки информации по электромагнитному каналу

Значения коэффициентов экранирования некоторых ограждающих конструкций приведены в табл. 1.

Таблица 1

Значения коэффициентов экранирования некоторых ограждающихконструкций на частотах 100, 500 и 1000 МГц
(по данным Гостехкомиссии)

№ п/п	Тип здания	Экранирование (дБ) (коэффициент экранирования $k_{экр}$) на частотах:		
		100 Мгц	500 МГц	1000 МГц
	Деревянное здание с толщиной стен 20 см:			
1	окно без решетки	5-7 (1,8-2,2)	7-9 (2,2-2,8)	9-11 (2,8-3,5)
2	окно закрыто решеткой с ячейкой 5 см	6-8 (2,0-2,5)	10-12 (3,2-4,0)	12-14 (4,0-5,0)
	Кирпичное здание с толщиной кирпичной стены 1,5 кирпича:			
3	окно без решетки	13-15 (4,5-5,6)	15-17 (5,6-7,0)	16-19 (6,3-8,9)
4	окно закрыто решеткой с ячейкой 5 см	17-19 (7,0-8,9)	20-22 (10,0-12,6)	22-25 (12,6-17,8)
	Железобетонные здания с ячейкой арматуры 15х15 см и толщиной 160 мм:			
5	окно без решетки	20-25 (10,0-17,8)	18-19 (8,0-8,9)	15-17 (5,6-7,0)
6	окно закрыто решеткой с ячейкой 5 см	28-32 (25,1-39,8)	23-27 (14,1-22,4)	20-25 (10,0-17,8)

Примечание: оконный проем составляет не более 30% от площади стены.

Напряженность электромагнитного поля E на границе контролируемой зоны вычисляется по следующей формуле:

$$E_{кз} = (E * k_з) / k_{экр} \text{ (мкВ/м)}, \quad (3)$$

где E - напряженность электромагнитного поля непосредственно у ПК;
$k_з$ - коэффициент затухания (2);
$k_{экр}$ - коэффициент экранирования (табл. 1).

Для практического рассчета оценки защищенности помещения от утечки по ПЭМИН необходимо определить максимальное значение отношения «сигнал/шум» - Δ, при котором исключается определение злоумышленником содержания (смысла) перехваченного сообщения, т.е. определить смысловой критерий безопасности сообщений.

Значение «сигнал/шум» - Δ рассчитывается на границе контролируемой

зоны, при котором сигналом является уровень электромагнитного излучения вокруг ПК, а шумом – напряженность поля атмосферных помех.

Специалистами в области защиты информации было рассчитано, что значение Δ не должно превышать:

$\Delta \leq 1$ (для важных информации);

$\Delta \leq 0{,}7$ (для особо важной информации)

Указанные значения Δ будут рассматриваться в данном практикуме без изучения методики расчета. Оптимальное значение Δ определяется на основании исследований, проведенных с помощью специальных измерительных инструментов.

Порядок выполнения работы:

Проведите расчет защищенности помещения от утечки информации по электромагнитному каналу. В качестве источника электромагнитного излучения возьмите ПК, расположенный на расстоянии R от границы контролируемой зоны (рис.1).

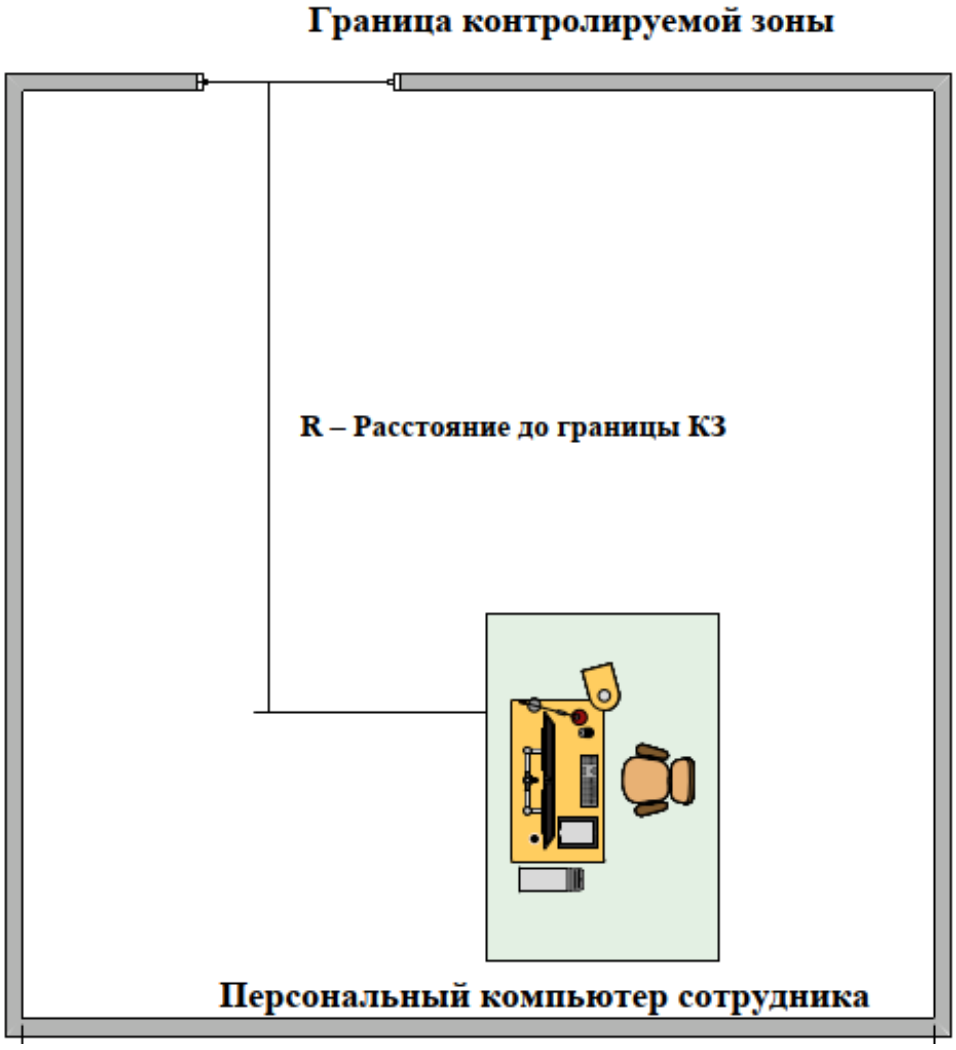

Рис. 1. План помещения

Для проведения расчетов необходимо учитывать значение напряженности электромагнитного поля, создаваемого ПК. При выполнении расчетов в реальных условиях необходимо учитывать пространственную диаграмма распределения интенсивности электрического поля вокруг ПК и использовать оборудование для измерения значений напряженности электромагнитного поля.

Пиповые значения напряженности электромагнитного поля $\boldsymbol{E}$, создаваемого ПК.

Таблица 2

Значения напряженности электромагнитного поля $\boldsymbol{E}$, создаваемого ПК

Номер	Значения электромагнитного поля $\boldsymbol{E}$ (мкВ/м) на частотах		
	100 МГц	500 МГц	1000 МГц
1.	510	1300	1300
2.	530	1350	1310
3.	550	1400	1320
4.	570	1450	1330
5.	590	1500	1350
6.	610	1550	1390
7.	630	1600	1400
8.	650	1520	1430
9.	670	1320	1450
10.	690	1420	1490

Проведите расчеты на основании исходных данных по вашему варианту и результаты внесите в таблицу:

Ход вычислений	Данные, полученные из таблиц или в результате расчетов, на частотах		
	100 МГц	500 МГц	1000 МГц
Значения электромагнитного поля E, создаваемого ПК, мкВ/м			
Значение коэффициента затухания kз			
Значение коэффициента экранирования kэкр			
Напряженность электромагнитного поля на границе контролируемой зоны			
Среднеквадратическое значение напряженности поля Eа атмосферных помех			
Отношение сигнал/шум на границе контролируемой зоны			

Вывод:

Среднеквадратические значения напряженности поля $\boldsymbol{E}$а атмосферных помех не расчитывать, считать одинаковыми для всех вариантов и равными:

	100 МГц	500 МГц	1000 МГц
Eа , мкВ/м (Tа=293^{o}K, fэкв=40 Мгц)	0,346	1,738	3,467

Варианты:

Номер варианта	$k_З = 1 / r^n$		$k_{экр}$ Таб. 1, пункт	E Таб. 2, пункт	Δ
	r	n			
1.	10	1,3	1	1	1
2.	11	1,4	2	2	1
3.	12	1,5	3	3	1
4.	13	1,6	4	4	1
5.	14	1,7	5	5	1
6.	15	1,8	6	6	1
7.	16	1,9	1	7	1
8.	17	2,0	2	8	1
9.	18	2,1	3	9	1
10.	19	2,2	4	10	1
11.	20	2,3	5	1	1
12.	10	2,4	6	2	0,7
13.	11	2,5	1	3	0,7
14.	12	2,6	2	4	0,7
15.	13	2,7	3	5	0,7
16.	14	2,8	4	6	0,7
17.	15	1,3	5	7	0,7
18.	16	1,4	6	8	0,7
19.	17	1,5	1	9	0,7
20.	18	1,6	2	10	0,7
21.	19	1,7	3	1	0,7
22.	20	1,8	4	2	0,7
23.	10	1,9	5	3	0,7
24.	15	2,0	6	4	0,7
25.	20	1,6	1	5	0,7

Приложение 2

Защита выделенного помещения от утечки по акустическому каналу

Таблица 1

Уровни интенсивности речи в октавных полосах и предельные спектры шумов [14]

Номер октавы	Средняя частота, $f_р$	Уровни речи и предельные спектры шумов, дБ								
		речь	ПС-20	ПС-25	ПС-30	ПС-35	ПС-40	ПС-45	ПС-50	ПС-55
1	250	67,9	31	35	40	45	49	54	59	63
2	500	66,9	24	29	34	39	44	49	54	25
3	1000	61,5	20	25	30	35	40	45	50	55
4	2000	57,0	17	22	27	32	37	42	47	52
5	4000	53,0	14	20	25	30	35	40	44	50
6	6000	48,5	13	18	23	28	33	38	43	49
Суммарные уровни, дБ		71	32,3	36,6	41,6	47	51	60	61	65
ПС-25 - кабинет при одном работающем; ПС-30 - библиотека; ПС-35 - комната для сна и отдыха; ПС-40 – кабинет без собственных шумов; ПС-45 - кабинет для умственной работы без собственных шумов; ПС-50 - кабинет для речевой и телефонной связи; ПС-55 - кабинет для конторского труда и цеховой администрации										

Таблица 2.

Уровни шумов, измеренные на частоте 1000 Гц[14]

Источник шума и место его измерения	Уровень шума, дБ (f = 1000Гц)
акустические шумы вне помещений:	
тихий сад	20

тихая улица (без движения транспорта)	30 - 35
обычный средний шум на улице	55 - 60
шумная улица без трамвайного движения	60 - 75
трамвай на расстоянии 10 -20 м	80 - 85
троллейбус на расстоянии 5 м	77
грузовой автомобиль в городе на расстоянии 10-20 м	60 - 75
легковой автомобиль в городе на расстоянии 10-20 м	50 - 65
электропоезд на эстакаде на расстоянии 6 м	90
акустические шумы в помещениях:	
обычное учреждение, жилое помещение	40
шепот на расстоянии 1 м	20-25
спокойный разговор 3 человек в комнате средних раз-меров	45-50
громкая музыка по радио	80
Разговор на расстоянии 1 м:обычный	55 - 60
громкий	65 - 70
громкий разговор по телефону	55
шумное собрание	65 - 70
коридоры	35 - 40
бухгалтерия без посетителей	30 - 35
комната шумная	40 - 50
комната тихая	25 - 30
кабинет при одном работающем	20 - 25

Таблица 3.

Зависимость между формантной ($А_ф$), слоговой (S) и словесной (W) разборчивостью[14]

*А*ф, отн. ед.	*S*, %	*W*, %	*А*ф, отн. ед.	*S*, %	*W*, %
0,05	5,0	30,0	0,55	84,0	98,5
0,10	15,0	63,0	0,60	87,0	98,8
0,15	26,0	76,0	0,65	90,0	99,0
0,20	36,0	85,0	0,70	92,5	99,2
0,25	46,0	90,0	0,75	95,2	99,4
0,30	54,0	93,0	0,80	96,5	99,6
0,35	62,5	94,5	0,85	98,0	99,7
0,40	69,0	96,0	0,90	99,0	99,8
0,45	75,0	97,0	0,95	99,5	99,9
0,50	80,0	98,0	1,00	100,0	100,0

Таблица 4

Значения коэффициентов разборчивости *w*,
соответствующие определенным уровням ощущения формант $E_ф$[14]

*E*ф, дБ	*w*, отн. ед.	*E*ф, дБ	*w*, отн. ед.	*E*ф, дБ	*w*, отн. ед.	*E*ф, дБ	*w*, отн. ед.
*E*ф < 15 *w* = 0		-8	0,040	9	0,50	26	0,960
		-7	0,050	12	0,60	27	0,970
		-6	0,060	15	0,70	28	0,980
		-5	0,075	18	0,80	29	0,985
-15	0,002	-4	0,095	19	0,83	30	0,990
-14	0,005	-3	0,110	20	0,86	33	0,995
-13	0,007	-2	0,140	21	0,88	36	1,000
-12	0,010	-1	0,17	22	0,900	*E*ф > 36 *w* = 1	
-11	0,015	0	0,20	23	0,915		
-10	0,020	3	0,30	24	0,930		
-9	0,030	6	0,40	25	0,945		

Таблица 5.

Градации понятности речи и соответствующие им значения формантной ($A_ф$), слоговой (S) и словесной (W) разборчивости [14]

Понятность	Разбочивость, %		
	форматная (*A*ф)	слоговая (*S*)	словестная (*W*)
Предельно допустимая	15-22	25-40	75-87
Удовлетворительная	22-31	40-44	87-93
Хорошая	31-50	44-80	93-98
Отличная	50 и выше	80 и выше	98 и выше

Таблица 6.

Разборчивость речи и уровни ощущения формант в октавных полосах[14]

$A_{ф.русск.} = 0{,}05 * (1{,}34w1 + 2{,}5\,w2 + 4{,}24w3 + 5{,}88\,w4 + 5w5 + 1{,}04w6)$							
		Средняя частота октавных полос, Гц					
		250	500	1000	2000	4000	6000
		Вклад частот в разборчивость формант, %					
		6,7	12,5	21,2	29,4	25	5,2
Понятность речи		Разборчивость речи в конкретнойоктавной полосе частот, ***w*i**					
		Уровень ощущения формант *E*ф. = *B*р. – *B*ш. в конкретной октавной полосе, дБ					
Смысл непонятен	< 15	0 <-12	0,015 -11	0,02 -10	0,03 -9	0,03 -9	0 <-12
Предельно допустимая	15 – 22	0,01 -12	0,02 -10	0,03 -9	0,04 -8	0,04 -8	0,007 <-12
Удовлетворительная	22 – 31	0,015 -11	0,03 -9	0,04 -8	0,06 -6	0,05 -7	0,011 -12
Хорошая	31 – 50	0,02 -10	0,04 -8	0,06 -6	0,09 -4	0,077 -5	0,016 -11
Отличная	>= 50	0,03 -9	0,06 -6	0,11 -3	0,147 -2	0,125 -2	0,026 -10

Таблица 7.

Значения коэффициентов звукоизоляции материалов и ограждающихконструкций [14]

Номер п/п	Материал или конструкция	Толщина, мм	Поверхностная плотность, кг/м^2	**Q**$_{пер}$, дБ
1.Стены и перегородки				
Стена из кирпичной кладки без штукатурки (из красного кирпича):				
1.1.	в 0,5 кирпича	120,0	204,0	48,0

1.2.	в 1 кирпич	250,0	425,0	53,0
1.3.	в 1,5 кирпича	380,0	646,0	44,0
1.4.	в 2 кирпича	520,0	884,0	25,0
1.5.	в 2,5 кирпича	640,0	1088,0	59,0
1.6.	Виброкирпичная панель, не ош-тукатуренная	140,0	240,0	49,5
1.7.	То же	160,0	280,0	50,4
1.8.	Стена из пустотелого кирпича	380,0	-	51,0
1.9.	То же	510,0	-	54,0
1.10.	Стена из железобетона	100,0	240,0	49,0
1.11.	То же	140,0	340,0	51,0
1.12.	То же	160,0	400,0	52,0
1.13.	То же	180,0	430,0	53,0
1.14.	То же	200,0	500,0	54,0
1.15.	То же	300,0	750,0	44,6
1.16.	То же	800,0	2000,0	62,8
1.17.	Гипсобетонная (гипсолитовая) плита	80,0	115,0	39,7
1.18.	То же	95,0	135,0	40,6
1.19.	Газобетонная плита	240,0	270,0	50,25
1.20.	Керамзитобетонная плита	80,0	100,0	39,0
1.21.	То же	100,0	150,0	41,2
1.22.	То же	120,0	195,0	42,6
1.23.	Шлакоблоки, оштукатуренные сдвух сторон	220,0	360,0	52,0
Шлакогипсовые стенные плиты:				
1.24.	2х5 см	130,	120,0	40,0

		0		
1.25.	2х6 см	170,0	150,0	42,0
Пемзобетонные стенные плиты:				
1.26.	2х6 см	150,0	135,0	40,0
1.27.	2х8,5 см	200,0	185,0	43,0
1.28.	Стены из пемзобетона	140,0	150,0	42,0
1.29.	То же	230,0	250,0	50,0
1.30.	Стена из шлакобетона	140,0	150,0	42,0
1.31.	То же	250,0	400,0	52,7
1.32.	То же из пустотелых пемзобе-тонных блоков	190,0	190,0	43,0
1.33.	То же	290,0	270,0	50,0
1.34.	Древесно-стружечная плита	20,0	12,0	27,4
1.35.	Перегородка одинарная из до-сок толщиной 2 см, оштукату-ренная с обеих сторон и окле-енная обоями	60,0	70,0	37,0
1.36.	Перегородка одинарная из до-сок толщиной 2,5 см, оштукату-ренная с обеих сторон по вой-локу	70,0	76,0	39,0
1.37.	Перегородка двойная из бру- сков 10 см, обшитых с двух сторон досками толщиной 2,5см и отштукатуренная с двух сторон	180,0	95,0	45,0
1.38.	То же с оштукатуркой по вой-локу	190,0	96,0	47,0
1.39.	Перегородка двойная из фанер-ных листов толщиной 3 мм с промежутком 2,5 см, заполнен-ным шлаковатой	30,0	8,0	26,0
1.40.	То же с промежутком 5 см	55,0	12,0	29,0

1.41.	То же с промежутком 6,5 см	70,0	14,0	34,0
1.42.	Гипсовые пустотелые камни толщиной 1 см с двумя стенка- ми толщиной по 1,5 см и про- межутком 8 см с засыпкой шла-ком	110,0	117,0	41,0
2. Окна				
2.1.	Одинарное остекление без уп-лотнительных прокладок	3,0	-	22,0
2.2.	Тоже	4,0	-	26,0
2.3.	Тоже	6,0	-	26,0
2.4.	Двойное остекление, расстоя-ние между стеклами 57 мм, беззвукопоглощающего материала(нар. - внутр.)	3,0/3,0	-	32,0
2.5.	То же со звукопоглощающим материалом	3,0/3,0	-	42,0
2.6.	Двойное остекление, расстоя-ние между стеклами 90 мм, беззвукопоглощающего материала	3,0/3,0	-	38,0
2.7.	То же со звукопоглощающим материалом	3,0/3,0	-	43,0
2.8.	Двойное остекление, расстоя-ние между стеклами 57 мм, беззвукопоглощающего материала	4,0/4,0	-	38,0
2.9.	То же со звукопоглощающим материалом	4,0/4,0	-	41,0
2.10.	Двойное остекление, расстоя-ние между стеклами 90 мм, беззвукопоглощающего материала	4,0/4,0	-	41,0
2.11.	Двойное остекление, расстоя-ние между стеклами 57 см, без звукопоглощающего материала	6,0/3,0	-	35,0
2.12.	Двойное остекление, расстоя-ние между стеклами 90 мм, беззвукопоглощающего материала	6,0/3,0	-	37,0

2.13.	Двойное остекление, расстояние между стеклами 38 мм, беззвукопоглощающего материала	6,0/6,0	-	40,0
2.14.	То же, 190 мм	6,0/6,0	-	45,0
2.15.	То же, 400 мм	6,0/6,0	-	48,0
3. Двери				
Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см:				
3.1.	без уплотняющих прокладок	-	-	18,0
3.2.	с уплотняющими прокладками	-	-	23,0
3.3.	То же, с обвязкой толщиной 2,5см и филенкой из 3 мм фанеры без уплотняющих прокладок	-	-	10,0
3.4.	То же, оклеенная фанерой раз-мером 90х200 см,без уплот-няющих прокладок	-	-	22,0
Глухая щитовая дверь толщиной 40 мм, облицованная с двух сторон фанерой толщиной 4 мм:				
3.5.	без уплотняющих прокладок	-	-	24,0
3.6.	с уплотняющими прокладками	-	-	32,0
Щитовая дверь из твердых древесно-волокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненная стекловатой:				
3.7.	без уплотняющих прокладок	-	-	30,0
3.8.	с уплотняющими прокладками	-	-	33,0
То же, заполненная минеральным войлоком:				
3.9.	без уплотняющих прокладок	-	-	28,0
3.10.	с уплотняющими прокладками	-	-	32,0
3.11.	Тяжелая дубовая дверь разме-ром 90х210 см, плотно при- гнанная	-	-	25,0
3.12.	Металлическая дверь (герме-тичная)	-	-	30,0

Порядок выполнения работы:

Необходимо рассчитать суммарную разборчивость формант в смежном помещении, коридоре и за наружной стеной. Сделайте выводы о возможности или невозможности утечки звуковой информации, необходимости использования дополнительных средств защиты выделенного помещения от утечки по акустическому каналу при необходимости. В расчетах

необходимо использовать табличные значения показателей, указанных в таблицах 3-9.

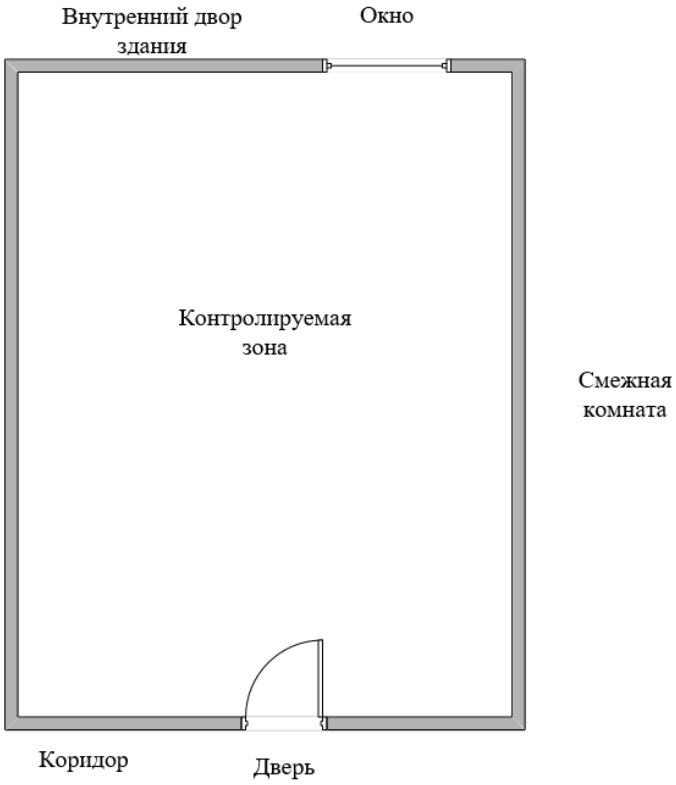

Рис. 2. Схема исследуемого кабинета

Значение $Q_{\text{пер.}}$ указано в табл. 3[14].

Номер октавы	Ср. частота, $f_р$	Уровни речи Речь, L1	Коэф. звукоизоляции с учетом повышения на частотах 4000, 6000 и понижения на частоте 250 на 6 дБ Qпер	$L1$ + 6 - $Q_{пер}$, дБ	$L2 = L$р, дБ
1.	250				
2.	500				
3.	1000				
4.	2000				
5.	4000				
6.	6000				

Номер октавы	Ср. частота, fр	L2 = Lр, дБ	Предельные спектры шумов ПС-45, Lш, дБ	Еф= Lр – Lш, дБ	Значения коэф. разборчивости wi по табл. 6
1.	250				
2.	500				
3.	1000				
4.	2000				
5.	4000				
6.	6000				

$A_{ф.русск.}$ = 0,05*(1,34w_1 + 2,5 w_2 + 4,24w_3 +5,88 w_4+5w_5+1,04w_6) =

Выводы:

Оценка защищенности от утечки речевой информации с возможностью прослушки на внешней стене.

Номер октавы	Ср. частота,*f*р	Уровни речи Речь, *L*1	Коэф. звукоизоляции с учетом повышения на частотах 4000, 6000 и понижения на частоте 250 на 6 дБ *Q*пер	*L*1 + 6 - *Q*пер, дБ	*L*2 = *L*р, дБ
1.	250	67,9			
2.	500	66,9			
3.	1000	61,5			
4.	2000	57,0			
5.	4000	53,0			
6.	6000	48,5			

Номер октавы	Ср. частота,*f*р	*L*2 = *L*р, дБ	Предельные спектрышумов ПС-35, Lш, дБ	*E*ф= *L*р – *L*ш, дБ	Значения коэф. разборчивости *w*i по табл. 3
1.	250				
2.	500				
3.	1000				
4.	2000				
5.	4000				
6.	6000				

По формуле (2) находим суммарную разборчивость

$A_{ф.русск.}$ = 0,05*(1,34w_1 + 2,5 w_2 + 4,24w_3 +5,88 w_4+5w_5+1,04w_6) =

Выводы:

Оценка защищенности от утечки речевой информации с возможностью прослушки в коридоре.

№ октавы	Ср. частота,*f*р	Уровниречи Речь, *L*1	Коэф. звукоизоляции с учетом повышения на частотах 4000, 6000 и понижения на частоте 250 на 6 дБ *Q*пер	*L*1 + 6 - *Q*пер, дБ	*L*2 = *L*р, дБ
1.	250				
2.	500				
3.	1000				
4.	2000				
5.	4000				

6.	6000				

№ октавы	Ср. частота, *f*р	L2 = Lр, дБ	Предельные спектры шумов ПС-35, Lш, дБ	Еф= Lр – Lш, дБ	Значения коэффициентов разборчивости *w*i по табл. 3
1.	250				
2.	500				
3.	1000				
4.	2000				
5.	4000				
6.	6000				

Определим суммарную разборчивость по формуле (3):

$A_{ф.русск.}$ = 0,05*(1,34w_1 + 2,5 w_2 + 4,24w_3 +5,88 w_4+5w_5+1,04w_6) =

Выводы:

На основании схемы типового помещения, рассмотренного в примере (рис. 2),

Уровни интенсивности речи в октавных полосах указаны в табл. 3, для всех вариантов они одинаковы.

Номер варианта	Смежное помещение	Наружная стена	Коридор
1.	Стена (табл. 9 п. 1.1) ПС-25 (табл. 3)	Стена (табл. 9 п. 1.2) Окно (табл. 9 п. 2.1) So = 40% ПС-35 (табл. 3)	Стена (табл. 9 п. 1.1) Дверь (табл. 9 п. 3.1) So = 20% ПС-25 (табл. 3)
2.	Стена (табл. 9 п. 1.6) ПС-30 (табл. 3)	Стена (табл. 9 п. 1.3) Окно (табл. 9 п. 2.2) So = 50% ПС-40 (табл. 3)	Стена (табл. 9 п. 1.6) Дверь (табл. 9 п. 3.2) So = 30% ПС-30 (табл. 3)
3.	Стена (табл. 9 п. 1.10) ПС-35 (табл. 3)	Стена (табл. 9 п. 1.4) Окно (табл. 9 п. 2.3) So = 60% ПС-45 (табл. 3)	Стена (табл. 9 п. 1.10) Дверь (табл. 9 п. 3.3) So = 20% ПС-35 (табл. 3)
4.	Стена (табл. 9 п. 1.17) ПС-40 (табл. 3)	Стена (табл. 9 п. 1.5) Окно (табл. 9 п. 2.4) So = 40% ПС-35 (табл. 3)	Стена (табл. 9 п. 1.17) Дверь (табл. 9 п. 3.4) So = 30% ПС-25 (табл. 3)
5.	Стена (табл. 9 п. 1.18) ПС-45 (табл. 3)	Стена (табл. 9 п. 1.7) Окно (табл. 9 п. 2.5) So = 50% ПС-40 (табл. 3)	Стена (табл. 9 п. 1.18) Дверь (табл. 9 п. 3.5) So = 20% ПС-30 (табл. 3)

6.	Стена (табл. 9 п. 1.20) ПС-50 (табл. 3)	Стена (табл. 9 п. 1.8) Окно (табл. 9 п. 2.6) So = 60% ПС-45 (табл. 3)	Стена (табл. 9 п. 1.20) Дверь (табл. 9 п. 3.6) So = 30% ПС-35 (табл. 3)
7.	Стена (табл. 9 п. 1.21) ПС-55 (табл. 3)	Стена (табл. 9 п. 1.9) Окно (табл. 9 п. 2.7) So = 40% ПС-35 (табл. 3)	Стена (табл. 9 п. 1.21) Дверь (табл. 9 п. 3.7) So = 20% ПС-25 (табл. 3)
8.	Стена (табл. 9 п. 1.22) ПС-30 (табл. 3);	Стена (табл. 9 п. 1.13) Окно (табл. 9 п. 2.8) So = 50% ПС-40 (табл. 3)	Стена (табл. 9 п. 1.22) Дверь (табл. 9 п. 3.8) So = 30% ПС-30 (табл. 3)
9.	Стена (табл. 9 п. 1.24) ПС-35 (табл. 3)	Стена (табл. 9 п. 1.14) Окно (табл. 9 п. 2.9) So = 60% ПС-45 (табл. 3)	Стена (табл. 9 п. 1.24) Дверь (табл. 9 п. 3.9) So = 20% ПС-35 (табл. 3)
10.	Стена (табл. 9 п. 1.25) ПС-40 (табл. 3)	Стена (табл. 9 п. 1.15) Окно (табл. 9 п. 2.10) So = 40% ПС-35 (табл. 3)	Стена (табл. 9 п. 1.25) Дверь (табл. 9 п. 3.10) So = 30% ПС-25 (табл. 3)
11.	Стена (табл. 9 п. 1.26) ПС-45 (табл. 3)	Стена (табл. 9 п. 1.16) Окно (табл. 9 п. 2.11) So = 50% ПС-40 (табл. 3)	Стена (табл. 9 п. 1.26) Дверь (табл. 9 п. 3.11) So = 20% ПС-30 (табл. 3)
12.	Стена (табл. 9 п. 1.30) ПС-35 (табл. 3)	Стена (табл. 9 п. 1.19) Окно (табл. 9 п. 2.12) So = 60% ПС-45 (табл. 3)	Стена (табл. 9 п. 1.30) Дверь (табл. 9 п. 3.1) So = 30% ПС-35 (табл. 3)
13.	Стена (табл. 9 п. 1.6) ПС-25 (табл. 3)	Стена (табл. 9 п. 1.27) Окно (табл. 9 п. 2.13) So = 40% ПС-35 (табл. 3)	Стена (табл. 9 п. 1.34) Дверь (табл. 9 п. 3.2) So = 20% ПС-25 (табл. 3)
14.	Стена (табл. 9 п. 1.35) ПС-30 (табл. 3)	Стена (табл. 9 п. 1.31) Окно (табл. 9 п. 2.14) So = 50% ПС-40 (табл. 3)	Стена (табл. 9 п. 1.35) Дверь (табл. 9 п. 3.3) So = 30% ПС-30 (табл. 3)
15.	Стена (табл. 9 п. 1.36) ПС-35 (табл. 3)	Стена (табл. 9 п. 1.23) Окно (табл. 9 п. 2.15) So = 60% ПС-45 (табл. 3)	Стена (табл. 9 п. 1.36) Дверь (табл. 9 п. 3.4) So = 20% ПС-35 (табл. 3)
16.	Стена (табл. 9 п. 1.37) ПС-25 (табл. 3)	Стена (табл. 9 п. 1.32) Окно (табл. 9 п. 2.1) So = 40% ПС-35 (табл. 3)	Стена (табл. 9 п. 1.17) Дверь (табл. 9 п. 3.5) So = 30% ПС-25 (табл. 3)

17.	Стена (табл. 9 п. 1.10) ПС-30 (табл. 3)	Стена (табл. 9 п. 1.3) Окно (табл. 9 п. 2.2) So = 50% ПС-40 (табл. 3)	Стена (табл. 9 п. 1.38) Дверь (табл. 9 п. 3.6) So = 20% ПС-30 (табл. 3)
18.	Стена (табл. 9 п. 1.30) ПС-35 (табл. 3)	Стена (табл. 9 п. 1.32) Окно (табл. 9 п. 2.3) So = 60% ПС-45 (табл. 3)	Стена (табл. 9 п. 1.39) Дверь (табл. 9 п. 3.7) So = 30% ПС-35 (табл. 3)
19.	Стена (табл. 9 п. 1.25) ПС-25 (табл. 3)	Стена (табл. 9 п. 1.23) Окно (табл. 9 п. 2.4) So = 40% ПС-35 (табл. 3)	Стена (табл. 9 п. 1.40) Дверь (табл. 9 п. 3.8) So = 20% ПС-25 (табл. 3)
20.	Стена (табл. 9 п. 1.41) ПС-30 (табл. 3)	Стена (табл. 9 п. 1.31) Окно (табл. 9 п. 2.5) So = 50% ПС-40 (табл. 3)	Стена (табл. 9 п. 1.41) Дверь (табл. 9 п. 3.9) So = 30% ПС-30 (табл. 3)
21.	Стена (табл. 9 п. 1.10) ПС-35 (табл. 3)	Стена (табл. 9 п. 1.19) Окно (табл. 9 п. 2.6) So = 60% ПС-45 (табл. 3)	Стена (табл. 9 п. 1.41) Дверь (табл. 9 п. 3.10) So = 20% ПС-35 (табл. 3)
22.	Стена (табл. 9 п. 1.40) ПС-55 (табл. 3)	Стена (табл. 9 п. 1.19) Окно (табл. 9 п. 2.12) So = 60% ПС-45 (табл. 3)	Стена (табл. 9 п. 1.17) Дверь (табл. 9 п. 3.2) So = 20% ПС-25 (табл. 3)
23.	Стена (табл. 9 п. 1.30) ПС-45 (табл. 3)	Стена (табл. 9 п. 1.27) Окно (табл. 9 п. 2.13) So = 40% ПС-35 (табл. 3)	Стена (табл. 9 п. 1.21) Дверь (табл. 9 п. 3.3) So = 30% ПС-30 (табл. 3)
24.	Стена (табл. 9 п. 1.42) ПС-30 (табл. 3)	Стена (табл. 9 п. 1.31) Окно (табл. 9 п. 2.14) So = 50% ПС-40 (табл. 3)	Стена (табл. 9 п. 1.37) Дверь (табл. 9 п. 3.4) So = 20% ПС-35 (табл. 3)
25.	Стена (табл. 9 п. 1.42) ПС-30 (табл. 3)	Стена (табл. 9 п. 1.23) Окно (табл. 9 п. 2.15) So = 60% ПС-45 (табл. 3)	Стена (табл. 9 п. 1.35) Дверь (табл. 9 п. 3.5) So = 30% ПС-25 (табл. 3)