МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»
Институт информационных технологий, машиностроения и автотранспорта

УТВЕРЖДАЮ
И.о. директора ИИТМА
_____ Жданов В.Л.
«31» августа 2026г.

Комплект оценочных материалов

Направление подготовки 10.04.01 Информационная безопасность
Направленность (профиль) - Организация и технология защиты информации

Присваиваемая квалификация «магистр»
Формы обучения Очно-заочная

Документ подписан усиленной
квалифицированной электронной подписью
Яковлев Алексей Николаевич
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "КУЗБАССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Т.Ф. ГОРБАЧЕВА"
008AC3F1D5F988C83BF589283F4A0208EB
Срок действия с 13.11.2025 до 06.02.2027

Кемерово 2026

ОГЛАВЛЕНИЕ

1. Паспорт базы оценочных материалов профессиональных компетенций

Компетенция компетенции	Наименование дисциплины	Курс, семестр	Тип задания	Номер задания из БТЗ
УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий	Управление проектами	1,1	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	1-2
			Задание закрытого типа на установление соответствия (проверяет эксперт)	3-4
			Задание закрытого типа на установление последовательности (проверяет эксперт)	5-6
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	9-10
	Производственная, Преддипломная практика	2,4	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	7-8
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора	11-12
УК-2 Способен управлять проектом на всех этапах его жизненного цикла	Управление проектами	1,2	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	13-14
			Задание закрытого типа на установление соответствия (проверяет эксперт)	15-16
			Задание закрытого типа на установление последовательности (проверяет эксперт)	17-18
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	21-22
	Производственная, Организационно-управленческая практика	2,4	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	19-20
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора	23-24
УК-3 Способен	Менеджмент	1,1	Задание закрытого типа с выбором одного/нескольких правильного	25-26

Компетенция компетенции	Наименование дисциплины	Курс, семестр	Тип задания	Номер задания из БТЗ
организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	профессиональной деятельности		ответа из предложенных	
			Задание закрытого типа на установление соответствия (проверяет эксперт)	29-30
			Задание закрытого типа на установление последовательности (проверяет эксперт)	33-34
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	39-40
	Управление проектами	1,2	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	27-28
			Задание закрытого типа на установление соответствия (проверяет эксперт)	31-32
			Задание закрытого типа на установление последовательности (проверяет эксперт)	35-36
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	41-42
	Производственная, Организационно-управленческая практика	2, 3	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	37-38
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора	43-44
УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	Иностранный язык в профессиональной деятельности	1,1-2	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	45-52
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	53-56
УК-5 Способен анализировать и учитывать разнообразие	Философские проблемы науки	1,2	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	57-60

Компетенция компетенции	Наименование дисциплины	Курс, семестр	Тип задания	Номер задания из БТЗ
культур в процессе межкультурного взаимодействия	и техники		Задание закрытого типа на установление соответствия (проверяет эксперт)	61-64
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	65-72
УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	Менеджмент профессиональной деятельности	1,1	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	73-74
			Задание закрытого типа на установление соответствия (проверяет эксперт)	75-76
			Задание закрытого типа на установление последовательности (проверяет эксперт)	77-78
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	79-80
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	Защищенные информационные системы	1,1	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	81-82
			Задание закрытого типа на установление соответствия (проверяет эксперт)	87-88
			Задание закрытого типа на установление последовательности (проверяет эксперт)	93-94
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	101-102
	Управление информационной безопасностью	1,1	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	83-84
			Задание закрытого типа на установление соответствия (проверяет эксперт)	89-90
			Задание закрытого типа на установление последовательности (проверяет эксперт)	95-96
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	103-104
	Технологии обеспечения	1,2	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	85-86

Компетенция компетенции	Наименование дисциплины	Курс, семестр	Тип задания	Номер задания из БТЗ
	информационной безопасности		Задание закрытого типа на установление соответствия (проверяет эксперт)	91-92
			Задание закрытого типа на установление последовательности (проверяет эксперт)	97-98
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	105-106
	Производственная, Проектно-технологическая практика	1,2	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	99-100
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных	107-108
ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности;	Защищенные информационные системы	1,1	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	109-110
			Задание закрытого типа на установление соответствия (проверяет эксперт)	117-118
			Задание закрытого типа на установление последовательности (проверяет эксперт)	125-126
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	135-138
	Проектирование систем (компонента системы) обеспечения информационной безопасности	2,3	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	113-114
			Задание закрытого типа на установление соответствия (проверяет эксперт)	121-122
			Задание закрытого типа на установление последовательности (проверяет эксперт)	129-130
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	143-144
	Информационная безопасность интернета вещей	2,3	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	115-116
			Задание закрытого типа на установление соответствия (проверяет эксперт)	123-124

Компетенция компетенции	Наименование дисциплины	Курс, семестр	Тип задания	Номер задания из БТЗ
			Задание закрытого типа на установление последовательности (проверяет эксперт)	131-132
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	145-146
	Технологии обеспечения информационной безопасности	1,2	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	111-112
			Задание закрытого типа на установление соответствия (проверяет эксперт)	119-120
			Задание закрытого типа на установление последовательности (проверяет эксперт)	127-128
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	139-142
	Производственная, Проектно-технологическая практика	1,2	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	133-134
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных	147-148
ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	Управление информационной безопасностью	1,1	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	149-150
			Задание закрытого типа на установление соответствия (проверяет эксперт)	153-154
			Задание закрытого типа на установление последовательности (проверяет эксперт)	157-158
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	163-166
	Организационно - распорядительная документация по обеспечению информационно	1,2	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	151-152
			Задание закрытого типа на установление соответствия (проверяет эксперт)	155-156
			Задание закрытого типа на установление последовательности (проверяет эксперт)	159-160

Компетенция компетенции	Наименование дисциплины	Курс, семестр	Тип задания	Номер задания из БТЗ
	й безопасности		Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	167-170
	Производственная, Проектно-технологическая практика	1,2	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	161-162
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных	171-172
ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок;	Основы научных исследований	1,1	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	173-174
			Задание закрытого типа на установление соответствия (проверяет эксперт)	175-176
			Задание закрытого типа на установление последовательности (проверяет эксперт)	177-178
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	181-182
	Производственная, Проектно-технологическая практика	1,2	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	179-180
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных	183-184
ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи.	Основы научных исследований	1,1	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	185-186
			Задание закрытого типа на установление соответствия (проверяет эксперт)	187-188
			Задание закрытого типа на установление последовательности (проверяет эксперт)	189-190
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	13-194
	Производственная, Проектно-технологическая практика	1,2	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	191-192
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных	195-196

Компетенция компетенции	Наименование дисциплины	Курс, семестр	Тип задания	Номер задания из БТЗ
ПК-1 Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений	Организация защиты объектов информатизации	2,3	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	197-200
			Задание закрытого типа на установление соответствия (проверяет эксперт)	201-206
			Задание закрытого типа на установление последовательности (проверяет эксперт)	207-210
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	213-218
	Производственная, Преддипломная практика	2,4	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	211-212
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора	219-220
ПК-2 Способен приводить аналитическое обоснование необходимости создания систем защиты информации	Организация защиты объектов информатизации	2,3	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	221-224
			Задание закрытого типа на установление соответствия (проверяет эксперт)	225-230
			Задание закрытого типа на установление последовательности (проверяет эксперт)	231-234
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	237-242
	Производственная, Преддипломная практика	2,4	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	235-236
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора	243-244
ПК-3 Владеет нормативно-методической базой обеспечения защиты сведений, составляющих	Государственная тайна и защита информации	2,3	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	245-248
			Задание закрытого типа на установление соответствия (проверяет эксперт)	249-254

Компетенция компетенции	Наименование дисциплины	Курс, семестр	Тип задания	Номер задания из БТЗ
государственную тайну			Задание закрытого типа на установление последовательности (проверяет эксперт)	255-258
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	263-268
	Производственная, Организационно-управленческая практика	2,3	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	259-260
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора	269-270
	Производственная, Преддипломная практика	2,4	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	261-262
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора	271-272
ПК-4 Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации	Организация защиты объектов информатизации	2,3	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	273-276
			Задание закрытого типа на установление соответствия (проверяет эксперт)	277-282
			Задание закрытого типа на установление последовательности (проверяет эксперт)	283-286
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	291-296
	Производственная, Организационно-управленческая практика	2,4	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	287-288
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора	297-298
	Производственная, Преддипломная	2,4	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	289-290
			Задания комбинированного типа с выбором одного/нескольких	299-300

Компетенция компетенции	Наименование дисциплины	Курс, семестр	Тип задания	Номер задания из БТЗ
	практика		правильного ответа из предложенных с последующим объяснением своего выбора	
ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ	Ввод системы защиты информации в эксплуатацию	2,3	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	301-302
			Задание закрытого типа на установление соответствия (проверяет эксперт)	305-306
			Задание закрытого типа на установление последовательности (проверяет эксперт)	309-310
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	317-320
	Организация приемочных испытаний системы защиты информации	2,3	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	303-304
			Задание закрытого типа на установление соответствия (проверяет эксперт)	307-308
			Задание закрытого типа на установление последовательности (проверяет эксперт)	311-312
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	321-324
	Производственная, Организационно-управленческая практика	2,4	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	313-314
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора	325-326
	Производственная, Преддипломная практика	2,4	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	315-316
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора	327-328
ПК-6	Построение моделей угроз	1,1	Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных	329-332

Компетенция компетенции	Наименование дисциплины	Курс, семестр	Тип задания	Номер задания из БТЗ
	информационной безопасности		Задание закрытого типа на установление соответствия (проверяет эксперт)	333-338
			Задание закрытого типа на установление последовательности (проверяет эксперт)	339-344
			Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)	349-356
	Производственная, Организационно-управленческая практика	2,3	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	345-346
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора	357-358
	Производственная, Преддипломная практика	2,4	Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)	347-348
			Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора	359-360

2. ТЕСТОВЫЕ ЗАДАНИЯ, ПОЗВОЛЯЮЩИЕ ОСУЩЕСТВЛЯТЬ ОЦЕНКУ КОМПЕТЕНЦИЙ С КЛЮЧАМИ К ОЦЕНИВАНИЮ

УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td colspan="5">Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных</td></tr>
<tr><td>2</td><td>1.</td><td>Управление проектами</td><td>К техникам модерации в проектной деятельности НЕ относится:
1. Мозговой штурм
2. Схема анализа проблемы
3. Блоки и параграфы</td><td>3</td></tr>
<tr><td>2</td><td>2.</td><td>Управление проектами</td><td>Смету проекта согласовывает и утверждает …
1. исполнитель
2. заказчик
3. оператор</td><td>2</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление соответствия (проверяет эксперт)</td></tr>
<tr><td>2</td><td>3.</td><td>Управление проектами</td><td>Соотнесите этап анализа ситуации с его описанием:<table><tr><td>Этап</td><td>Описание</td></tr><tr><td>A. Определение ключевых проблем</td><td>1. Установка направления для поиска решения</td></tr><tr><td>B. Построение карты заинтересованных сторон</td><td>2. Выявление влияния участников на проблему</td></tr><tr><td>C. Формулировка целей анализа</td><td>3. Оценка причин возникновения затруднений в проекте</td></tr><tr><td>D. Сбор информации</td><td>4. Получение фактических данных о ситуации</td></tr></table></td><td>A-3, B-2, C-1, D-4</td></tr>
<tr><td>2</td><td>4.</td><td>Управление проектами</td><td>Соотнесите стадию выработки стратегии с её примером:<table><tr><td>Стадии</td><td>Примеры</td></tr></table></td><td>A-3, B-2, C-1, D-4</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td><table>
<tr><td>A. Постановка цели</td><td>1. Выявить возможные задержки в реализации решения</td></tr>
<tr><td>B. Поиск альтернатив</td><td>2. Внедрить новый инструмент планирования или улучшить текущий</td></tr>
<tr><td>C. Оценка рисков</td><td>3. Повысить эффективность взаимодействия в команде</td></tr>
<tr><td>D. Выбор оптимального варианта</td><td>4. Остановиться на стратегии, дающей максимальный эффект</td></tr>
</table></td><td></td></tr>
<tr><td colspan="5">Задание закрытого типа на установление последовательности (проверяет эксперт)</td></tr>
<tr><td>2</td><td>5.</td><td>Управление проектами</td><td>Установите правильную последовательность этапов критического анализа проблемной ситуации в проекте:
1. Определение проблемы
2. Сбор и анализ информации
3. Формулирование причин возникновения проблемы
4.Поиск возможных решений</td><td>2, 1, 4, 3</td></tr>
<tr><td>2</td><td>6.</td><td>Управление проектами</td><td>Расположите этапы разработки стратегии действий при решении проблемной ситуации:
1. Генерация альтернатив
2. Выявление целей
3. Выбор оптимального решения
4. Оценка рисков</td><td>2, 1, 4, 3</td></tr>
<tr><td colspan="5">Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)</td></tr>
<tr><td>4</td><td>7.</td><td>Производственная, Преддипломная практика</td><td>Сотрудники компании начали массово использовать незащищенные мессенджеры для передачи рабочих файлов, так как корпоративная почта имеет жесткий лимит на объем вложений.</td><td>Провести системный анализ (бизнес-потребности и риски ИБ). Стратегия: внедрение корпоративного облачного хранилища с разграничением прав доступа вместо блокировок, мешающих работе.</td></tr>
<tr><td>4</td><td>8.</td><td>Производственная, Преддипломная практика</td><td>Выявлено дублирование функций между отделом ИТ и службой ИБ при управлении учетными записями, что приводит к задержкам.</td><td>Разработка стратегии централизации управления через внедрение IdM-системы и четкое разделение зон ответственности в регламенте</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
2	9.	Управление проектами	Процесс, в ходе которого навыки, инструменты и технологии используются для планирования, выполнения, отслеживания и завершения проектов в установленные сроки, называется …	Управление проектом
2	10.	Управление проектами	Анализ … среды включает изучение влияния экономики, правового регулирования и управления, политических процессов, природной среды и ресурсов, социальной и культурной составляющих общества, научно-техническое и технологическое развитие общества, инфраструктуры и т.п.	Внешней
Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора				
4	11.	Производственная, Преддипломная практика	«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования вы выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Выбор этого варианта демонстрирует системный подход: выявлена проблемная ситуация (уязвимость стены и отсутствие СЗИ) и выработана логическая стратегия действий от обследования до аттестации
4	12.	Производственная, Преддипломная практика	В компании внедрена новая система безопасности, которая требует смены пароля каждые 15 дней. Это привело к тому, что сотрудники стали записывать пароли на стикерах. Какая стратегия действий будет системно верной? 1. Штрафовать сотрудников за хранение записей на рабочем столе. 2. Отменить требование регулярной смены паролей. 3. Внедрить аппаратную двухфакторную аутентификацию (токены) или биометрию, снизив частоту смены паролей. 4. Купить более яркие стикеры, чтобы пароли было проще находить.	3 Системный подход требует анализа «человеческого фактора». Стратегия должна устранять корень проблемы (неудобство), а не бороться с симптомами. Использование токенов обеспечивает безопасность без создания когнитивной нагрузки на персонал.

УК-2 Способен управлять проектом на всех этапах его жизненного цикла

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td colspan="5">Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных</td></tr>
<tr><td>2</td><td>13.</td><td>Управление проектами</td><td>Какие факторы необходимо учитывать в процессе принятия решения о реализации инвестиционного проекта?
1. инфляцию, риски, альтернативные варианты инвестирования;
2. инфляцию и политическую ситуацию в стране;
3. инфляцию, уровень безработицы и альтернативные варианты инвестирования.</td><td>1</td></tr>
<tr><td>2</td><td>14.</td><td>Управление проектами</td><td>Для оценки жизнеспособности проекта сравнивают варианты проекта с точки зрения:
1. сроков реализации;
2. их финансовой реализуемости;
3. простоты реализации;
4. отсутствия рисков.</td><td>1</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление соответствия (проверяет эксперт)</td></tr>
<tr><td>2</td><td>15.</td><td>Управление проектами</td><td>Установите соответствие между этапом жизненного цикла проекта и его описанием:<table><tr><td>Этап</td><td>Описание</td></tr><tr><td>A. Инициация</td><td>1. Разработка целей, сроков, бюджета</td></tr><tr><td>B. Планирование</td><td>2. Принятие решения о старте проекта</td></tr><tr><td>C. Реализация</td><td>3. Выполнение проектных работ</td></tr><tr><td>D. Завершение</td><td>4. Формальное окончание проекта</td></tr></table></td><td>2, 1, 3, 4</td></tr>
<tr><td>2</td><td>16.</td><td>Управление проектами</td><td>Установите соответствие между документом и этапом, где он используется:<table><tr><td>Документ</td><td>Этап</td></tr><tr><td>A. Устав проекта</td><td>1. Планирование</td></tr><tr><td>B. План управления</td><td>2. Инициация</td></tr></table></td><td>2, 1, 3, 4</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			C. Отчёт о ходе работ — 3. Реализация D. Финальный отчёт — 4. Завершение	
Задание закрытого типа на установление последовательности (проверяет эксперт)				
2	17.	Управление проектами	Расположите этапы жизненного цикла проекта в правильной последовательности: 1. Реализация 2. Инициация 3. Планирование 4. Завершение	2, 3, 1, 4
2	18.	Управление проектами	Установите последовательность действий при запуске проекта: 1. Формирование команды 2. Постановка целей проекта 3. Определение ресурсов 4. Разработка графика работ	2, 3, 1, 4
Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)				
4	19.	Производственная, Организационно-управленческая практика	Организация инициирует проект по модернизации системы защиты персональных данных в связи с изменениями в законодательстве. Опишите ваши действия как менеджера проекта на этапе инициации.	Разработка и утверждение Устава проекта. Необходимо определить: глобальную цель, ключевые заинтересованные стороны, предварительный бюджет и сроки.
4	20.	Производственная, Организационно-управленческая практика	Организация инициирует проект по модернизации системы защиты персональных данных в связи с изменениями в законодательстве. Опишите ваши действия как менеджера проекта на этапе завершения этого проекта.	Проведение приемо-сдаточных испытаний и подписание актов. Формирование итогового отчета, расформирование проектной команды, передача системы в эксплуатацию.
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
2	21.	Управление проектами	План реализации проекта содержит наименование этапа, сроки, длительность выполнения и …… за каждую работу.	ответственных
2	22.	Управление проектами	Концепция проекта состоит из следующих элементов: резюме, …, план реализации, финансовый план, оценка эффективности.	бюджет
Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора				
4	23.	Производственная, Организационно-	На этапе завершения проекта по созданию защищенной системы Заказчик подписал все акты, но требует бесплатно добавить в систему функцию,	3 Управление жизненным циклом

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
		управленческая практика	которой не было в Техническом задании (ТЗ). Как поступить менеджеру проекта? 1. Бесплатно выполнить требование Заказчика, чтобы не портить с ним отношения. 2. Отказать Заказчику в грубой форме, сославшись на закрытие проекта. 3. Объяснить Заказчику, что проект завершен согласно ТЗ, и предложить оформить новое требование как отдельный проект (или через процедуру управления изменениями). 4. В тайне от руководства поручить программистам дописать требуемую функцию.	проекта требует жесткого соблюдения его границ. Выполнение работ вне ТЗ без оформления доп. соглашений ведет к неконтролируемым затратам ресурсов.
4	24.	Производственная, Организационно-управленческая практика	Во время этапа планирования проекта внедрения СЗИ выяснилось, что выделенного бюджета не хватает на закупку сертифицированного оборудования. Ваши действия? 1. Закупить более дешевое несертифицированное оборудование и скрыть это от Заказчика. 2. Инициировать совещание со стейкхолдерами для пересмотра бюджета проекта или сокращения его масштаба (границ) без потери качества защиты. 3. Начать проект и надеяться, что в процессе появятся дополнительные деньги. 4.Поручить разработчикам написать бесплатный аналог СЗИ своими силами за те же сроки.	2 На этапе планирования при обнаружении дефицита бюджета менеджер обязан вынести проблему на уровень спонсоров/заказчиков проекта для принятия стратегического решения, а не идти на нарушение требований безопасности.

УК-3 Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных				
1	25.	Менеджмент профессиональной деятельности	Типовая система управления включает: 1. аппаратно-программный комплекс поддержки коммуникаций; 2.организационная структура и роли в проекте; 3. информационная система сопровождения проекта.	2
1	26.	Менеджмент профессиональной деятельности	Самый большой плюс этой формы организации предпринимательского дела - простота регистрации 1. ИП 2. ООО 3. ПАО	1

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td>2</td><td>27.</td><td>Управление проектами</td><td>Менеджмент, осуществляемый посредством создания и функционирования управленческих команд как одна из форм коллективного управления, основан на процессе делегирования полномочий. Это …
1. инновационный менеджмент;
2. командный менеджмент;
3. финансовый менеджмент</td><td>2</td></tr>
<tr><td>2</td><td>28.</td><td>Управление проектами</td><td>Одной из составляющих командного менеджмента является внешняя среда. Так ли это? …
1. да
2. нет</td><td>2</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление соответствия (проверяет эксперт)</td></tr>
<tr><td>1</td><td>29.</td><td>Менеджмент профессиональной деятельности</td><td>Установите соответствие аспектов предпринимательства с их описаниями<table><tr><td>А. Экономический</td><td>1. Предпринимателю для осуществления новых комбинаций в условиях риска необходим определенный набор личностных свойств</td></tr><tr><td>Б. Личностный</td><td>2. Предприниматель осуществляет организацию или реорганизацию хозяйственного механизма путем соединения факторов производства с целью получения максимальной вывод в каждой конкретной ситуации</td></tr><tr><td>В. Управленческий финансовый, психологический и социальный риск</td><td>3. Предприниматель осуществляет целенаправленное новаторское воздействие на производственный процесс, его координацию, берет на себя весь риск</td></tr></table></td><td>А-2, Б-1, В-3</td></tr>
<tr><td>1</td><td>30.</td><td>Менеджмент профессиональной деятельности</td><td>Соотнесите тип коммерческой организации с её характеристикой<table><tr><td>А. ИП</td><td>1. Уставной капитал разделен на доли в соответствии с учредительным договором</td></tr><tr><td>Б. ООО</td><td>2. Полная гарантия, что при выходе участников капитал не изымается</td></tr><tr><td>В. АО</td><td>3. Возможность использовать УСН и оплачивать налоги по упрощенной схеме</td></tr></table></td><td>А-3, Б-1, В-2</td></tr>
<tr><td>2</td><td>31.</td><td>Управление проектами</td><td>Соотнесите виды мотивации в командной деятельности с их</td><td>А-4, Б-3, В-2, Г-1</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td>характеристиками:<table><tr><td>А. Отрицательная мотивация</td><td>1. мотивация, основанная на стимулах поощрения</td></tr><tr><td>Б. Устойчивая мотивация</td><td>2. мотивация, которая требует постоянной внешней поддержки</td></tr><tr><td>В. Неустойчивая мотивация</td><td>3. мотивация, основанная на естественных потребностях человека</td></tr><tr><td>Г. Положительная мотивация</td><td>4. мотивация, основанная на стимулах наказания</td></tr></table></td><td></td></tr>
<tr><td>2</td><td>32.</td><td>Управление проектами</td><td>Установите соответствие между командной ролью и её функцией:<table><tr><td>Командная роль</td><td>Функция</td></tr><tr><td>А. Лидер</td><td>1. Выполняет конкретные задания и задачи</td></tr><tr><td>В. Генератор идей</td><td>2. Предлагает новые решения и подходы</td></tr><tr><td>С. Исполнитель</td><td>3. Определяет направление, управляет процессом</td></tr><tr><td>D. Контролёр</td><td>4. Следит за сроками и качеством выполнения работы</td></tr></table></td><td>A-3, B-2, C-1, D-4</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление последовательности (проверяет эксперт)</td></tr>
<tr><td>1</td><td>33.</td><td>Менеджмент профессиональной деятельности</td><td>Установите последовательность этапов проектной деятельности:
1.Целеполагание;
2. Реализация проекта;
3. Сдача проекта и презентация;
4. Проблематизация;
5. Планирование;
6. Завершение.</td><td>4, 1, 5, 2, 3, 6</td></tr>
<tr><td>1</td><td>34.</td><td>Менеджмент профессиональной деятельности</td><td>Расположите этапы проектной деятельности в правильной последовательности:
1.Целеполагание;
2. Реализация проекта;
3. Сдача проекта и презентация;
4. Проблематизация;
5. Планирование;
6. Завершение.</td><td>4, 1, 5, 2, 3, 6</td></tr>
<tr><td>2</td><td>35.</td><td>Управление проектами</td><td>Расположите в правильной последовательности первые буквы английских</td><td>S-M-A-R-T</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			слов, являющихся аббревиатурой названия технологии постановки целей: «Measurable» - измеримый, «Specific» - специфичный, конкретный, «Relevant» - актуальный; «Achievable» - достижимый, «Time-bound» - ограниченный во времени	
2	36.	Управление проектами	Конфликты в командной работе происходят по схеме: $X_1+X_2=X_3$. Расположите в верной последовательности значения X_i 1. Конфликтная ситуация 2. конфликт 3. инцидент	1, 3, 2
Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)				
3	37.	Производственная, Организационно-управленческая практика	Вы назначены руководителем временной рабочей группы из 4 человек (аналитик, два инженера и специалист по режимам). Ваша цель – за 2 недели подготовить филиал к аттестации. Из-за сжатых сроков в команде возникло напряжение и споры о приоритетах. Сформулируйте командную стратегию.	параллельное выполнение задач с ежедневными 10-минутными совещаниями для контроля статуса и снятия блокирующих проблем.
3	38.	Производственная, Организационно-управленческая практика	Вы назначены руководителем временной рабочей группы из 4 человек (аналитик, два инженера и специалист по режимам). Ваша цель – за 2 недели подготовить филиал к аттестации. Из-за сжатых сроков в команде возникло напряжение и споры о приоритетах. Распределите задачи.	Аналитик: Актуализирует и собирает разрешительную и техническую документацию на автоматизированную систему. Инженеры: установка, настройка и проверка корректности работы СЗИ от НСД и антивирусов. Специалист по режимам: Проверяет физическую безопасность помещений, опечатывание техники и ведение журналов учета.
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
1	39.	Менеджмент профессиональной деятельности	Коэффициент ликвидности показывает _____ фирмы	Платежеспособность
1	40.	Менеджмент профессиональной деятельности	К теоретическим методам исследования относятся: …	Анализ
2	41.	Управление проектами	Процесс разделения проекта на несколько этапов, подразумевающий регулярное взаимодействие с заинтересованными сторонами и постоянное улучшение на каждом этапе отвечает … методологии.	гибкой
2	42.	Управление проектами	Приложение знаний, навыков, инструментов и методов к операциям проекта для удовлетворения требований, предъявляемых к проекту, это …	управление проектом

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора				
3	43.	Производственная, Организационно-управленческая практика	Команда из 5 специалистов должна за неделю провести аудит безопасности крупного филиала. Из-за сжатых сроков в коллективе началась паника. Какую стратегию руководства выбрать? 1. Сказать команде работать по 14 часов в сутки без выходных. 2. Разбить крупную цель на мелкие ежедневные задачи, распределить зоны ответственности согласно сильным сторонам сотрудников и проводить утренние 10-минутные летучки. 3. Выполнить большую часть работы самостоятельно, чтобы показать пример. 4. Отменить аудит и доложить руководству, что сроки нереальные.	2 Эффективное руководство командой в условиях стресса требует декомпозиции целей и четкого распределения ролей, что снижает неопределенность и структурирует работу коллектива.
3	44.	Производственная, Организационно-управленческая практика	В вашей проектной команде опытный инженер-проектировщик отказывается документировать свои решения, заявляя, что «и так всё работает, а писанина – пустая трата времени». Ваши действия как лидера? 1. Уволить инженера за невыполнение требований. 2. Согласиться с ним, так как работающая система важнее бумаг. 3. Объяснить инженеру системные риски для всей команды в случае его ухода или болезни и сделать документирование обязательным критерием приемки его работы . 4. Поручить документирование за него менее опытному стажеру.	3 Лидер команды должен выработать общие правила игры. Документирование - это не бюрократия, а обеспечение непрерывности процессов и снижение зависимости команды от одного человека.

УК-4 Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных				
1	45.	Иностранный язык в профессиональной деятельности	Children under five years old _____ swim without an adult. A) have to B) must not C) are supposed to D) may	B
1	46.	Иностранный язык в профессиональной деятельности	three hundred and ninty-nine A) 587 B) 399 C) 458	B
1	47.	Иностранный язык в профессиональной	What is demand? A) Demand is the quantity of a good that buyers wish to buy at each price	A

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
		деятельности	B) Demand is the quantity of a good that sellers wish to sell at each price	
1	48.	Иностранный язык в профессиональной деятельности	My father ___ at work. A) is B) am C) are	A
2	49.	Иностранный язык в профессиональной деятельности	Last summer we ... (live) in the country and (go) to the river everyday. A) will live; went B) lived; went C) have lived; went	B
2	50.	Иностранный язык в профессиональной деятельности	You should be ashamed of ___! You took candy from a baby. A) ourselves B) yourself C) himself D) itself	B
2	51.	Иностранный язык в профессиональной деятельности	We ___ got a cat. A) have B) has	A
2	52.	Иностранный язык в профессиональной деятельности	People should buy security systems for ___ homes in order to prevent break-ins. A) their B) we C) us D) itselves	A
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
1	53.	Иностранный язык в профессиональной деятельности	Answer the question. What language is spoken in Poland?	Polish
1	54.	Иностранный язык в профессиональной деятельности	What is the plural of the word “businessman”?	Businessmen
2	55.	Иностранный язык в профессиональной деятельности	Answer the question. What is the opposite of the verb “to remember”?	To forget
2	56.	Иностранный язык в профессиональной деятельности	Answer the question. Which of the following is misspelt: comparison, commerceal, complicated, convenient?	Commerceal

УК-5 Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td colspan="5">Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных</td></tr>
<tr><td>2</td><td>57.</td><td>Философские проблемы науки и техники</td><td>Понятие, противоположное по смыслу «истине» в гносеологии:
1. пропаганда;
2. заблуждение;
3. суждение;
4. предрассудок;
5. иллюзия.</td><td>2</td></tr>
<tr><td>2</td><td>58.</td><td>Философские проблемы науки и техники</td><td>В каком методе познания процедура измерения определённых характеристик изучаемой системы является неотъемлемой частью?
1. только в наблюдении;
2. и в наблюдении и в эксперименте;
3. только в эксперименте;
4. нет правильного ответа.</td><td>3</td></tr>
<tr><td>2</td><td>59.</td><td>Философские проблемы науки и техники</td><td>Научная теория, занимающаяся проблемами поиска человеком истинных фактов бытия в целом и природы в частности, называется…
1. теорией хаоса;
2. натуральной философией;
3. космологией;
4. теорией познания.</td><td>4</td></tr>
<tr><td>2</td><td>60.</td><td>Философские проблемы науки и техники</td><td>Как называется метод эмпирического познания, при котором изучаемое явление ставится в особые, специфические и варьируемые условия?
1. измерение;
2. эксперимент;
3. наблюдение.</td><td>2</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление соответствия (проверяет эксперт)</td></tr>
<tr><td>2</td><td>61.</td><td>Философские проблемы науки и техники</td><td>Установите соответствие между определениями метода научного познания и самим методом
<table><tr><td>А. Активное, целенаправленное, строго контролируемое воздействие исследователя на изучаемый объект</td><td>1. наблюдение</td></tr><tr><td>Б. Чувственное отражение предметов и явлений внешнего мира</td><td>2. измерение</td></tr><tr><td>В. Определение количественных значений свойств, сторон изучаемого объекта или явления с помощью специальных технологических устройств</td><td>3. эксперимент</td></tr></table></td><td>А-3, Б-1, В-2</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>2</td><td>62.</td><td>Философские проблемы науки и техники</td><td>Какое определение истины соответствует исторической эпохе?<table><tr><td>А. XXв.</td><td>1. Истина – это открывающаяся сущность вещи</td></tr><tr><td>Б. Средние века</td><td>2. Истина – это проявление идеи (Платон) или сущности (Аристотель)</td></tr><tr><td>В. Новое время</td><td>3. Бог, вот что является истиной</td></tr><tr><td>Г. Античность</td><td>4. Истина – это соответствие чувств и идей фактам</td></tr></table></td><td>А-1, Б-3, В-2, Г-4</td></tr>
<tr><td>2</td><td>63.</td><td>Философские проблемы науки и техники</td><td>Определите, какому периоду времени присущи те или иные исторические формы науки<table><tr><td>А. неклассический</td><td>1. XX в.</td></tr><tr><td>Б. романтический</td><td>2. XVII в.</td></tr><tr><td>В. классический</td><td>3. XV в.</td></tr><tr><td>Г. постнеклассический</td><td>4. XXI в.</td></tr></table></td><td>А-1, Б-3, В-2, Г-4</td></tr>
<tr><td>2</td><td>64.</td><td>Философские проблемы науки и техники</td><td>Определите, какие исторические формы науки были в следующие периоды времени<table><tr><td>1. XX в.</td><td>А. неклассический</td></tr><tr><td>2. XVII в.</td><td>Б. романтический</td></tr><tr><td>3. XV в.</td><td>В. классический</td></tr><tr><td>4. XXI в.</td><td>Г. постнеклассический</td></tr></table></td><td>1-А, 2-В, 3-Б, 4-Г</td></tr>
<tr><td colspan="5">Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)</td></tr>
<tr><td>2</td><td>65.</td><td>Философские проблемы науки и техники</td><td>Исходной основой всех знаний о природе в древности являлись знания: …</td><td>физические</td></tr>
<tr><td>2</td><td>66.</td><td>Философские проблемы науки и техники</td><td>Свойство научного знания, связанное с постоянной проверкой полученных результатов, называется: …</td><td>достоверность</td></tr>
<tr><td>2</td><td>67.</td><td>Философские проблемы науки и техники</td><td>Какая из естественных наук первой достигла теоретической зрелости? …</td><td>механика</td></tr>
<tr><td>2</td><td>68.</td><td>Философские проблемы науки и техники</td><td>Как называется неадекватное представление о действительности, обусловленное ограниченностью общественно-исторической практики и знания? …</td><td>заблуждение</td></tr>
<tr><td>2</td><td>69.</td><td>Философские проблемы</td><td>Цель наблюдения и эксперимента – давать науке …</td><td>факты</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
		науки и техники		
2	70.	Философские проблемы науки и техники	Какое понятие Т. Кун определил словами: «некумулятивные эпизоды развития науки, во время которых старая парадигма замещается целиком или частично новой парадигмой, несовместимой со старой»? …	научная революция
2	71.	Философские проблемы науки и техники	Учение о способах и приёмах определённого вида деятельности это …	методология
2	72.	Философские проблемы науки и техники	Как называется то, что противостоит субъекту в его предметно-практической и познавательной деятельности? …	объект

УК-6 Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td colspan="5">Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных</td></tr>
<tr><td>1</td><td>73.</td><td>Менеджмент профессиональной деятельности</td><td>Для эффективного распределения времени целесообразно:
1. Распределить дела по блокам;
2. Составить список дел на неделю;
3. Знать свои ресурсы времени.</td><td>3</td></tr>
<tr><td>1</td><td>74.</td><td>Менеджмент профессиональной деятельности</td><td>Критерием результата и достижимости цели могут быть:
1. Полнота жизни;
2. Активный процесс деятельности;
3. Измеримость.</td><td>3</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление соответствия (проверяет эксперт)</td></tr>
<tr><td>1</td><td>75.</td><td>Менеджмент профессиональной деятельности</td><td>Установите соответствие:<table><tr><td>1. Перфекционизм</td><td>А. Становление, рост, интеграция и реализация в профессиональном труде профессиональных знаний и умений, профессионально значимых личностных качеств, мотивов и способностей, а также активное качественное преобразование человеком своего внутреннего мира, приводящее к принципиально новому его строю и способу жизнедеятельности – творческой самореализации в профессии - это профессиональное…</td></tr><tr><td>2. Адепт</td><td>Б. Человек, уже вставший на путь приверженности профессии и осваивающий ее – это не мастер, не авторитет, а…</td></tr></table></td><td>А-3, Б-2, В-1</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			3. Развитие — В. Диагностика проблем нерационального управления временем предполагает три уровня: и определение технической ошибки, определение внешних факторов и определение психологических препятствий. Среди психологических препятствий выделяют: несформулированность приоритетов; постоянная работа на пределе своих возможностей; страх вынужденного бездействия; боязнь успеха; страх нарушить существующее положение вещей, а также ЭТО. Иногда ЭТО называют «болезненным стремлением к безупречности».	
1	76.	Менеджмент профессиональной деятельности	Соотнесите термины с определениями А. Самострахование — 1. процесс страхования риска от возможных потерь путем переноса риска изменения цены с одного лица на другое лицо Б. Страхование — 2. передача определенных рисков страховой компании В. Хеджирование — 3. процесс распределения капитала между различными объектами вложения, которые непосредственно не связаны между собой Г. Диверсификация — 4. децентрализованная форма создания резервных фондов, обеспечивающая гибкость управления рисками и сохранение контроля над денежными средствами	А-4, Б-2, В-1, Г-3
Задание закрытого типа на установление последовательности (проверяет эксперт)				
1	77.	Менеджмент профессиональной деятельности	Установите последовательность метода мозгового штурма: 1. Формирование задачи; 2. Оценка результата; 3. Генерация идей во время групповой проработки поставленной задачи; 4. Комбинирование идей; 5. Планирование.	1, 3, 4, 5, 2
1	78.	Менеджмент профессиональной	Установите последовательность метода мозгового штурма: 1. Формирование задачи;	1, 3, 4, 5, 2

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
		деятельности	2. Оценка результата; 3. Генерация идей во время групповой проработки поставленной задачи; 4. Комбинирование идей; 5. Планирование.	
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
1	79.	Менеджмент профессиональной деятельности	Столкновение сторон, мнений, сил, любые виды борьбы между индивидами, цель которых – достижение (либо сохранение) средств производства, экономической позиции, власти или других ценностей, пользующихся общественным признанием, а также завоевание, нейтрализация либо устранение действительного (или мнимого) противника – это …	конфликт
1	80.	Менеджмент профессиональной деятельности	Способность быстро осваивать профессиональные новшества и новые специальности – это профессиональная …	мобильность

ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных				
1	81.	Защищенные информационные системы	Какой этап является первоочередным при обосновании состава требований к защищенной информационной системе (ЗИС) в проекте ТЗ? 1. Закупка лицензий на программное обеспечение. 2. Идентификация защищаемых активов и моделирование угроз безопасности. 3. Назначение администраторов системы. 4. Выбор поставщика офисной техники.	2
1	82.	Защищенные информационные системы	Какое проектное решение в ТЗ обосновывается необходимостью защиты информации от несанкционированного доступа при подключении системы к сетям общего пользования (Интернет)? 1. Установка дополнительных модулей оперативной памяти. 2. Применение межсетевого экранирования и средств построения VPN. 3. Регулярная очистка кэша браузера. 4. Увеличение скорости печати принтеров.	2
1	83.	Управление информационной безопасностью	Какой процесс в управлении ИБ является первичным для обоснования выбора мер защиты и формирования требований в техническом задании? 1. Закупка оборудования. 2. Оценка рисков информационной безопасности.	2

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td>3. Написание должностных инструкций.
4. Проведение инвентаризации мебели в офисе.</td><td></td></tr>
<tr><td>1</td><td>84.</td><td>Управление информационной безопасностью</td><td>При разработке ТЗ требование к «минимизации прав доступа», когда пользователю предоставляются только те полномочия, которые необходимы для выполнения работы, обосновывается принципом:
1. Максимальной открытости.
2. Производственной необходимости (наименьших привилегий).
3. Удобства администрирования.
4. Экономии оперативной памяти.</td><td>2</td></tr>
<tr><td>2</td><td>85.</td><td>Технологии обеспечения информационной безопасности</td><td>Какой этап является определяющим при обосновании требований к системе обеспечения информационной безопасности (СОИБ) в техническом задании?
1. Закупка серверного оборудования.
2. Анализ рисков и моделирование угроз безопасности информации.
3. Назначение системного администратора.
4. Выбор цвета интерфейса программного обеспечения.</td><td>2</td></tr>
<tr><td>2</td><td>86.</td><td>Технологии обеспечения информационной безопасности</td><td>Каким государственным стандартом (ГОСТ) следует руководствоваться в первую очередь при разработке структуры и содержания технического задания на создание автоматизированной системы?
1. ГОСТ 2.105 (Общие требования к текстовым документам).
2. ГОСТ 34.602 (Техническое задание на создание автоматизированной системы).
3. ГОСТ Р 7.0.97 (Организационно-распорядительная документация).
4. ГОСТ 19.101 (Виды программных документов).</td><td>2</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление соответствия (проверяет эксперт)</td></tr>
<tr><td>1</td><td>87.</td><td>Защищенные информационные системы</td><td>Установите соответствие свойств защищенности и технологий их обеспечения при обосновании ТЗ<table><tr><td>Свойство информации</td><td>Технологическое решение в проекте</td></tr><tr><td>А) Конфиденциальность</td><td>1) Резервное копирование и дублирование серверов</td></tr><tr><td>Б) Целостность</td><td>2) Использование алгоритмов симметричного шифрования</td></tr><tr><td>В) Доступность</td><td>3) Применение электронной подписи и хэш-функций</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
<tr><td>1</td><td>88.</td><td>Защищенные информационные системы</td><td>Установите соответствие этапов проектирования и действий по разработке ТЗ<table><tr><td>Этап раз работки</td><td>Действие проектировщика</td></tr></table></td><td>А - 2, Б - 3, В - 1</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><td>А) Обследование объекта</td><td>1) Согласование документа с заказчиком и регуляторами</td></tr><tr><td>Б) Формирование требований</td><td>2) Определение границ системы и состава ценных активов</td></tr><tr><td>В) Утверждение ТЗ</td><td>3) Определение класса защищенности системы по ГОСТ /ФСТЭК</td></tr></table></td><td></td></tr>
<tr><td>1</td><td>89.</td><td>Управление информационной безопасностью</td><td>Установите соответствие методов обработки рисков и проектных решений в ТЗ<table><tr><td>Метод обработки риска</td><td>Техническое/организационное решение в ТЗ</td></tr><tr><td>А) Снижение (минимизация)</td><td>1) Отказ от использования облачных сервисов для хранения гостайны</td></tr><tr><td>Б) Передача (перекладывание)</td><td>2) Внедрение системы двухфакторной аутентификации и шифрования</td></tr><tr><td>В) Уклонение (избегание)</td><td>3) Заключение договора страхования киберрисков или аутсорсинг ИБ</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
<tr><td>1</td><td>90.</td><td>Управление информационной безопасностью</td><td>Установите соответствие документов по управлению ИБ и их роли при разработке ТЗ<table><tr><td>Документ</td><td>Роль в обосновании требований</td></tr><tr><td>А) Политика ИБ</td><td>1) Описание конкретных векторов атак для выбора средств защиты</td></tr><tr><td>Б) Модель угроз</td><td>2) Фундамент, определяющие общие принципы и цели защиты</td></tr><tr><td>В) Техническое задание</td><td>3) Детальный перечень требований к реализации системы защиты</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td>2</td><td>91.</td><td>Технологии обеспечения информационной безопасности</td><td>Установите соответствие технологий защиты и решаемых ими задач при обосновании проекта<table><tr><td>Технология защиты</td><td>Основная задача обеспечения ИБ</td></tr><tr><td>А VPN (Virtual Private Network)</td><td>1) Обеспечение конфиденциальности данных при передаче по открытым каналам</td></tr><tr><td>Б) IDS/IPS системы</td><td>2) Обнаружение и предотвращение попыток внедрения вредоносного кода</td></tr><tr><td>В) Межсетевой экран (Firewall)</td><td>3) Регулирование доступа к ресурсам на сетевом уровне</td></tr></table></td><td>А - 3, Б - 1, В - 2.</td></tr>
<tr><td>2</td><td>92.</td><td>Технологии обеспечения информационной безопасности</td><td>Установите соответствие видов угроз и технологий их нейтрализации для обоснования ТЗ<table><tr><td>Вид угрозы</td><td>Технология нейтрализации</td></tr><tr><td>А) Несанкционированный доступ</td><td>1) Резервное копирование избыточное хранение (RAID)</td></tr><tr><td>Б) Модификация данных</td><td>2) Многофакторная аутентификация и управление доступом</td></tr><tr><td>В) Нарушение доступности</td><td>3) Использования электронной подписи (ЭП) и хэширования</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление последовательности (проверяет эксперт)</td></tr>
<tr><td>1</td><td>93.</td><td>Защищенные информационные системы</td><td>Расположите действия проектировщика по обоснованию состава средств защиты в логическом порядке:
1. Выбор конкретных защитных технологий (криптография, межсетевые экраны, антивирусы).
2. Построение модели угроз и определение актуальных векторов атак.
3. Оценка эффективности выбранных мер и их соответствие нормативным актам (ФСТЭК/ФСБ).
4. Определение класса защищенности информационной системы на основе категории данных.</td><td>4, 2, 1, 3.</td></tr>
<tr><td>1</td><td>94.</td><td>Защищенные информационные системы</td><td>Расставьте этапы процедуры обоснования требований к надежности защищенной системы:
1. Выбор технических решений для обеспечения бесперебойности (кластеризация, RAID, ИБП).
2. Анализ допустимого времени простоя системы при возникновении сбоев</td><td>2, 3, 1, 4.</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			или атак. 3. Определение количественных показателей надежности (время наработки на отказ). 4. Описание регламента резервного копирования и восстановления данных.	
1	95.	Управление информационной безопасностью	Установите правильную последовательность этапов управления рисками для обоснования требований к системе защиты: 1. Выбор мер и средств защиты для нейтрализации угроз. 2. Идентификация информационных активов и их ценности. 3. Анализ и оценка вероятности реализации угроз. 4. Определение остаточного риска после внедрения мер.	2, 3, 1, 4.
1	96.	Управление информационной безопасностью	Расставьте уровни нормативного обоснования требований к системе ИБ в порядке убывания их приоритетности (от общегосударственных к локальным): 1. Корпоративные инструкции и регламенты организации. 2. Федеральные законы и указы Президента РФ. 3. Отраслевые стандарты и требования регуляторов (ФСТЭК/ФСБ). 4. Политика информационной безопасности предприятия.	2, 3, 4, 1.
2	97.	Технологии обеспечения информационной безопасности	Установите правильную последовательность этапов разработки технического задания на создание системы обеспечения информационной безопасности (СОИБ) согласно ГОСТ 34.602: 1. Согласование и утверждение проекта ТЗ заказчиком и разработчиком. 2. Сбор и анализ исходных данных об объекте информатизации. 3. Формирование технических требований к подсистемам защиты. 4. Определение целей создания и назначения будущей системы.	2, 4, 3, 1.
2	98.	Технологии обеспечения информационной безопасности	Расположите действия инженера по обоснованию состава средств защиты в логической последовательности: 1. Выбор конкретных технологий защиты (шифрование, МЭ, антивирус). 2. Определение перечня актуальных угроз безопасности информации. 3. Сопоставление выбранных технологий с требованиями регуляторов (ФСТЭК/ФСБ). 4. Идентификация защищаемых активов и информационных потоков.	4, 2, 1, 3.
Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)				
2	99.	Производственная, Проектно-технологическая практика	Кейс-задача: «Организация защищенного удаленного доступа к корпоративной сети». Руководство компании приняло решение перевести ИТ-отдел на удаленный режим работы. Вам, как специалисту по защите информации, поручено реализовать проект по обеспечению безопасности этого процесса.	Для защиты данных при передаче через интернет необходимо использовать технологию VPN. Это обосновано необходимостью создания защищенного канала между домашним

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			Задание: Обоснуйте выбор технологии доступа и сформулируйте одно ключевое требование для раздела ТЗ «Технические требования».	ПК и офисом.
2	100.	Производственная, Проектно-технологическая практика	Кейс-задача: «Внедрение системы защиты от утечек (DLP) в юридическом департаменте». В юридическом департаменте крупной компании участились случаи случайной пересылки конфиденциальных договоров на личные адреса сотрудников. Вам поручено проработать вопрос внедрения системы контроля почтового трафика. Задание: Обоснуйте необходимость внедрения DLP-системы для почты и сформулируйте одно требование к функционалу для ТЗ.	Юридическая документация содержит коммерческую тайну и персональные данные. Утечка таких сведений грозит компании репутационными рисками и штрафами. DLP-система необходима для автоматического блокирования писем, содержащих ключевые слова (например, «Договор №», «Конфиденциально»).
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
1	101.	Защищенные информационные системы	При обосновании требований к системе защиты процесс присвоения информационной системе определенной категории (класса) в зависимости от уровня значимости обрабатываемой информации называется _____ защищенности.	определение класса (или классификация / категорирование).
1	102.	Защищенные информационные системы	Требования к системе, определяющие конкретные защитные функции (например, идентификация, аутентификация, управление доступом), называются _____.	функциональными требованиями
1	103.	Управление информационной безопасностью	Основной процесс управления ИБ, результатом которого является перечень недопустимых последствий и обоснование необходимости внедрения конкретных мер защиты в ТЗ, называется оценка _____.	рисков
1	104.	Управление информационной безопасностью	Высокоуровневый документ организации, на основе которого формулируются общие требования к проектируемой системе защиты и определяются цели обеспечения безопасности, называется _____ информационной безопасности.	политика
2	105.	Технологии обеспечения информационной безопасности	Процесс выявления актуальных угроз и оценки вероятности их реализации, проводимый для обоснования состава системы защиты в проекте, называется _____.	моделированием угроз
2	106.	Технологии обеспечения информационной безопасности	Требования к СОИБ, описывающие конкретные защитные действия системы (например, фильтрация трафика или шифрование данных), называются _____.	функциональными требованиями

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных				
2	107.	Производственная, Проектно-технологическая практика	«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберете правильный ответ и объясните свой выбора. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2
2	108.	Производственная, Проектно-технологическая практика	«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

ОПК-2 Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных				
1	109.	Защищенные информационные системы	Выберите компоненты, которые обычно входят в состав подсистемы управления доступом при разработке технического проекта защищенной системы: (Выбор нескольких ответов) 1. Механизмы идентификации и аутентификации пользователей. 2. Средства пожаротушения в серверной. 3. Средства разграничения прав доступа к ресурсам (файлам, БД). 4. Средства регистрации и учета событий безопасности (логирование). 5. Система кондиционирования воздуха.	1, 3, 4.
1	110.	Защищенные информационные системы	Какие графические документы обязательно разрабатываются в рамках технического проекта системы обеспечения информационной безопасности по ГОСТ 34.201-89? (**Выбор нескольких ответов**) 1. Схема структурная системы защиты. 2. Фотография фасада здания офиса. 3. Схема автоматизации (или схема соединений компонентов СЗИ). 4. План эвакуации при пожаре.	1, 3.
2	111.	Технологии обеспечения информационной безопасности	Какой этап является первоочередным при обосновании состава требований к системе обеспечения информационной безопасности в проекте ТЗ? 1. Закупка лицензий на программное обеспечение. 2. Идентификация активов и моделирование угроз безопасности. 3. Назначение системного администратора организации. 4 Обучение пользователей работе с офисными программами.	2
2	112.	Технологии обеспечения информационной безопасности	В какой раздел технического задания (согласно ГОСТ 34.602) включаются требования по обеспечению конфиденциальности, целостности и доступности информации? 1. Общие сведения о проекте. 2. Порядок контроля и приемки системы. 3. Требования к системе (или подсистемам защиты). 4. Требования к документированию.	3
3	113.	Проектирование систем (компонента системы) обеспечения информационной безопасности	На каком этапе проектирования системы обеспечения ИБ осуществляется построение модели угроз и определение актуальных векторов атак? 1. Ввод системы в эксплуатацию. 2. Гарантийное обслуживание. 3. Предпроектное обследование и формирование требований.	3

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td>4. Утилизация компонентов системы.</td><td></td></tr>
<tr><td>3</td><td>114.</td><td>Проектирование систем (компонента системы) обеспечения информационной безопасности</td><td>Какое проектное решение направлено на минимизацию ущерба при компрометации одного из сегментов корпоративной сети?
1. Использование антивируса на сервере.
2. Резервное копирование баз данных.
3. Сегментация сети с использованием межсетевых экранов.
4. Назначение одного администратора для всех подсистем.</td><td>3</td></tr>
<tr><td>3</td><td>115.</td><td>Информационная безопасность интернета вещей</td><td>При разработке технического проекта системы защиты промышленного интернета вещей (IIoT) для изоляции критически важных контроллеров от офисной сети предприятия рекомендуется использовать:
1. Одноранговую сеть (P2P) без маршрутизации.
2. Сегментацию сети с помощью виртуальных локальных сетей (VLAN) и межсетевых экранов.
3. Общую Wi-Fi сеть с открытым доступом для удобства обслуживания.
4. Прямое подключение каждого контроллера к сети Интернет через выделенный IP.</td><td>2</td></tr>
<tr><td>3</td><td>116.</td><td>Информационная безопасность интернета вещей</td><td>Что является обязательным этапом при разработке технического проекта системы обеспечения ИБ для IoT в соответствии с системным подходом?
1. Закупка самого дорогого оборудования на рынке.
2. Моделирование угроз и идентификация уязвимостей компонентов системы.
3. Личное собеседование с каждым пользователем системы.
4. Отказ от использования облачных технологий в пользу бумажных носителей.</td><td>2</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление соответствия (проверяет эксперт)</td></tr>
<tr><td>1</td><td>117.</td><td>Защищенные информационные системы</td><td>Установите соответствие видов проектной документации и их содержания<table><tr><td>Документ проекта</td><td>Содержание документа</td></tr><tr><td>А) Схема структурная СОИБ</td><td>1) Обоснование выбранных программ и устройств</td></tr><tr><td>Б) Спецификация оборудования</td><td>2) Иерархия и связи между компонентами защиты</td></tr><tr><td>В) Пояснительная записка</td><td>3) Перечень моделей, версий и количества закупаемых СЗИ</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
<tr><td>1</td><td>118.</td><td>Защищенные информационные системы</td><td>Установите соответствие уровней защиты и применяемых технологий в проекте<table><tr><td>Уровень защиты</td><td>Применяемая технология</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td><table>
<tr><td>А) Сетевой уровень</td><td>1) Биометрическая идентификация на рабочих станциях</td></tr>
<tr><td>Б) Системный уровень</td><td>2) Сегментация сети и межсетевое экранирование</td></tr>
<tr><td>В) Пользовательский уровень</td><td>3) Контроль прав доступа к файловым объектам ОС</td></tr>
</table></td><td></td></tr>
<tr><td>2</td><td>119.</td><td>Технологии обеспечения информационной безопасности</td><td>Установите соответствие классов средств защиты информации (СЗИ) и их проектных задач<table>
<tr><td>Класс СЗИ</td><td>Основная задача в техническом проекте</td></tr>
<tr><td>А) СЗИ от несанкционированного доступа (НД)</td><td>1) Обнаружение и блокировка сетевых угроз на периметре</td></tr>
<tr><td>Б) Межсетевой экран (МЭ)</td><td>2) Контроль доступа к файлам и устройствам внутри ОС</td></tr>
<tr><td>В) Система обнаружения вторжений (СОВ)</td><td>3) Анализ сетевого трафика и обнаружение атак (сигнатурных и аномальных)</td></tr>
</table></td><td>А - 2, Б - 1, В - 3.</td></tr>
<tr><td>2</td><td>120.</td><td>Технологии обеспечения информационной безопасности</td><td>Установите соответствие уровней архитектуры системы и применяемых технологий защиты<table>
<tr><td>Уровень системы</td><td>Технология защиты в проекте</td></tr>
<tr><td>А) Сетевой уровень</td><td>1) Разграничение прав доступа к таблицам БД</td></tr>
<tr><td>Б) Прикладной уровень</td><td>2) Проверка подлинности пользователя по биометрии</td></tr>
<tr><td>В) Уровень идентификации</td><td>3) Организация защищённого туннеля (VPN)</td></tr>
</table></td><td>А - 3, Б - 1, В - 2.</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td>3</td><td>121.</td><td>Проектирование систем (компонента системы) обеспечения информационной безопасности</td><td>Установите соответствие между стадией создания автоматизированной системы в защищенном исполнении (согласно ГОСТ 34.601-90) и основным содержанием работ на этой стадии:<table><tr><td>Стадия проектирования</td><td>Содержание работ</td></tr><tr><td>А) Формирование требований</td><td>1) Разработка деталей, схем и программных кодов</td></tr><tr><td>Б) Технический проект</td><td>2) Обследование объекта и создание обоснования необходимости системы</td></tr><tr><td>В) Рабочая документация</td><td>3) Разработка окончательных проектных решений по системе и её частям</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
<tr><td>3</td><td>122.</td><td>Проектирование систем (компонента системы) обеспечения информационной безопасности</td><td>При разработке технического проекта системы защиты информации соотнесите вид обеспечения (левая колонка) с его компонентами (правая колонка):<table><tr><td>Вид обеспечения СЗИ</td><td>Компоненты в проекте</td></tr><tr><td>А) Программное обеспечение</td><td>1) Инструкции и интерфейсы администратора и регламенты управления доступом</td></tr><tr><td>Б) Техническое обеспечение</td><td>2) Средства антивирусной защиты и операционные системы</td></tr><tr><td>В) Организационное обеспечение</td><td>3) Межсетевые экраны, серверы и средства криптозащиты</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
<tr><td>3</td><td>123.</td><td>Информационная безопасность интернета вещей</td><td>Установите соответствие между типом устройства (левая колонка) и его основной функцией в техническом проекте системы обеспечения информационной безопасности IoT (правая колонка):<table><tr><td>Тип устройств</td><td>Основная защитная функция</td></tr><tr><td>А. Криптографический модуль</td><td>1. Инспекция пакетов и сегментация трафика между IoT-сегментом и внешней сетью</td></tr><tr><td>Б. Межсетевой экран</td><td>2. Безопасное хранение ключей и выполнение доверенных</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><td></td><td>вычислений на устройствах</td></tr><tr><td>В. Система IDS/IPS</td><td>3. Обнаружение аномалий в поведении датчиков и попыток сканирования сети</td></tr></table></td><td></td></tr>
<tr><td>3</td><td>124.</td><td>Информационная безопасность интернета вещей</td><td>При разработке проекта защиты IoT-системы выберите соответствующий механизм защиты для каждой категории угроз:<table><tr><td>Категория угрозы</td><td>Механизм защиты в проекте</td></tr><tr><td>А) Подмена данных в канале связи</td><td>1) Контроль целостности прошивки</td></tr><tr><td>Б) Несанкционированный запуск вредоносного ПО</td><td>2) Двусторонняя аутентификация и шифрование</td></tr><tr><td>В) Перебор паролей к устройству</td><td>3) Ограничение количества попыток входа и использование сертификатов</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление последовательности (проверяет эксперт)</td></tr>
<tr><td>1</td><td>125.</td><td>Защищенные информационные системы</td><td>Расставьте этапы подготовки спецификации оборудования и программного обеспечения в составе технического проекта:
1. Проверка совместимости выбранных средств защиты с системным ПО.
2. Изучение перечня сертифицированных СЗИ, соответствующих требуемому классу защищенности.
3. Расчет необходимого количества лицензий и единиц аппаратных средств.
4. Оформление итоговой ведомости (спецификации) по установленной форме.</td><td>2, 1, 3, 4.</td></tr>
<tr><td>1</td><td>126.</td><td>Защищенные информационные системы</td><td>Установите правильную последовательность этапов разработки технического проекта системы обеспечения информационной безопасности (СОИБ):
1 Разработка структурной схемы системы защиты и схем соединений.
2. Выбор конкретных программно-аппаратных средств защиты (брендов и моделей СЗИ).
3. Составление пояснительной записки с техническим обоснованием решений.
4. Анализ требований утвержденного технического задания (ТЗ).</td><td>4, 2, 1, 3.</td></tr>
<tr><td>2</td><td>127.</td><td>Технологии обеспечения информационной безопасности</td><td>Расположите действия проектировщика по созданию подсистемы управления доступом в логическом порядке:
1. Выбор метода аутентификации (пароль, токен, биометрия).
2. Определение перечня защищаемых ресурсов и категорий пользователей.</td><td>2, 3, 1, 4.</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			3. Описание правил разграничения доступа (матрица доступа). 4. Проектирование механизмов регистрации (логирования) действий пользователей.	
2	128.	Технологии обеспечения информационной безопасности	Установите последовательность этапов проектирования защищенного канала связи (VPN) между офисами: 1. Выбор криптографических алгоритмов и протоколов (например, IPsec или TLS). 2. Определение точек входа/выхода трафика (места установки шлюзов). 3. Расчет необходимой пропускной способности канала с учетом шифрования. 4. Описание порядка генерации и распределения ключей шифрования.	2, 3, 1, 4.
3	129.	Проектирование систем (компонента системы) обеспечения информационной безопасности	Текст задания: Расположите этапы проектирования подсистемы управления доступом в логическом порядке (от анализа к реализации): 1. Определение перечня защищаемых информационных ресурсов. 2. Выбор программно-аппаратных средств идентификации и аутентификации. 3. Формирование матрицы доступа (назначение прав пользователям). 4. Разработка регламентов и инструкций по управлению учетными записями.	1, 3, 2, 4.
3	130.	Проектирование систем (компонента системы) обеспечения информационной безопасности	Установите правильную последовательность действий при разработке раздела «Моделирование угроз» в составе технического проекта: 1. Определение актуальных угроз безопасности информации. 2. Описание характеристик объекта информатизации и его границ. 3. Анализ потенциальных нарушителей (внутренних и внешних). 4. Оценка возможных негативных последствий (ущерба).	2, 3, 1, 4.
3	131.	Информационная безопасность интернета вещей	Установите правильную последовательность этапов разработки технического проекта системы обеспечения информационной безопасности (СОИБ) для сети Интернета вещей: 1. Выбор конкретных средств защиты информации и алгоритмов шифрования. 2. Проведение инвентаризации активов и идентификация IoT-устройств. 3. Моделирование угроз и определение векторов атак на компоненты системы. 4. Формирование требований к системе защиты и определение зон доверия. 5. Оценка остаточных рисков и составление спецификации оборудования.	2, 3, 4, 1, 5.
3	132.	Информационная безопасность интернета вещей	Расположите уровни модели взаимодействия устройств в IoT-системе (от оконечного устройства к пользователю) для корректного проектирования мер защиты на каждом этапе: 1. Облачная платформа или центр обработки данных (аналитика и хранение). 2. Полевой уровень (датчики, исполнительные механизмы, контроллеры).	2, 3, 1, 4.

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			3. Уровень передачи данных (шлюзы, маршрутизаторы, сетевые протоколы). 4. Приложение пользователя (интерфейс мониторинга и управления).	
Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)				
2	133.	Производственная, Проектно-технологическая практика	Кейс-задача: «Организация защищенного удаленного доступа к корпоративной сети». Руководство компании приняло решение перевести ИТ-отдел на удаленный режим работы. Вам, как специалисту по защите информации, поручено реализовать проект по обеспечению безопасности этого процесса. Задание: Разработайте концептуальную схему размещения оборудования. Где именно в сети должен находиться VPN-шлюз?	VPN-шлюз следует разместить в качестве пограничного устройства между интернетом и внутренней сетью. Он должен находиться перед внутренним межсетевым экраном, чтобы трафик проверялся до попадания в основной сегмент сети.
2	134.	Производственная, Проектно-технологическая практика	Кейс-задача: «Внедрение системы защиты от утечек (DLP) в юридическом департаменте». В юридическом департаменте крупной компании участились случаи случайной пересылки конфиденциальных договоров на личные адреса сотрудников. Вам поручено проработать вопрос внедрения системы контроля почтового трафика. Задание: Определите место установки DLP-шлюза в сетевой инфраструктуре. Как он должен взаимодействовать с почтовым сервером?	DLP-шлюз следует интегрировать с корпоративным почтовым сервером по протоколу SMTP (в разрыв) или через Smart Host. Почтовый сервер должен перенаправлять все исходящие сообщения на DLP-шлюз для анализа перед их фактической отправкой во внешнюю сеть.
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
1	135.	Защищенные информационные системы	Графический документ, отображающий состав подсистем защиты, их распределение по узлам информационной системы и связи между ними, называется _____ системы обеспечения ИБ.	структурная **схема**
1	136.	Защищенные информационные системы	При проектировании защищенной системы метод разграничения доступа, при котором права пользователя определяются его ролью или должностными обязанностями, называется _____.	ролевое управление доступом
1	137.	Защищенные информационные системы	Проектное решение, предполагающее создание защищенного логического канала поверх общедоступной сети связи для объединения сегментов системы, называется технологией _____.	VPN (или виртуальная частная сеть).
1	138.	Защищенные информационные системы	Стадия проектирования, на которой обосновываются окончательные технические решения по системе защиты и формируется полный комплект документации для её реализации, называется _____.	технический проект
2	139.	Технологии обеспечения информационной	Графический документ, отображающий состав подсистем защиты, их взаимную связь и распределение по узлам сети, называется _____	структурная схема

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
		безопасности	системы обеспечения ИБ.	
2	140.	Технологии обеспечения информационной безопасности	Раздел технического проекта, содержащий перечень всех программных и аппаратных средств защиты с указанием их точных наименований, версий и количества, называется _____.	спецификация
2	141.	Технологии обеспечения информационной безопасности	Технология создания защищенного логического канала поверх незащищенной сети (например, Интернета) для объединения офисов в единую сеть называется _____.	VPN (или виртуальная частная сеть).
2	142.	Технологии обеспечения информационной безопасности	Основной текстовый документ технического проекта, в котором приводится детальное описание и техническое обоснование всех принятых проектных решений, - это _____.	пояснительная записка.
3	143.	Проектирование систем (компонента системы) обеспечения информационной безопасности	Как называется основной документ, разрабатываемый на начальном этапе проектирования, который содержит совокупность требований к системе и является юридическим основанием для выполнения работ исполнителем?	Техническое задание (или ТЗ).
3	144.	Проектирование систем (компонента системы) обеспечения информационной безопасности	Процесс описания потенциального нарушителя, его возможностей, целей и вероятных способов реализации атак в рамках разработки проекта системы защиты называется _____ угроз.	Моделирование
3	145.	Информационная безопасность интернета вещей	Перечислите три основных уровня (сегмента) типовой архитектуры системы Интернета вещей (IoT), которые необходимо учитывать при разработке технического проекта системы обеспечения информационной безопасности.	Восприятие, сетевой, прикладной
3	146.	Информационная безопасность интернета вещей	Как называется специализированный сетевой узел, который в проектах систем защиты IoT-решений выполняет роль посредника между оконечными устройствами (датчиками) и облачной платформой, обеспечивая локальную фильтрацию трафика и трансляцию протоколов?	Шлюз
Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных				
2	147.	Производственная, Проектно-технологическая практика	«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями	2

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			регуляторов? Выберете правильный ответ и объясните свой выбора. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	
2	148.	Производственная, Проектно-технологическая практика	«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	3

ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных				
1	149.	Управление информационной	Какой локальный нормативный акт является документом верхнего уровня в системе управления ИБ и служит базой для разработки всех остальных	2

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td>безопасностью</td><td>организационно-распорядительных документов?
1. Инструкция по антивирусной защите.
2. Политика информационной безопасности.
3. Журнал учета машинных носителей.
4. Приказ о назначении системного администратора.</td><td></td></tr>
<tr><td>1</td><td>150.</td><td>Управление информационной безопасностью</td><td>Каким распорядительным документом в организации официально вводится в действие проект разработанного «Положения о защите персональных данных»?
1. Служебной запиской.
2. Приказом руководителя.
3. Протоколом совещания.
4. Трудовым договором.</td><td>2</td></tr>
<tr><td>2</td><td>151.</td><td>Организационно-распорядительная документация по обеспечению информационной безопасности</td><td>Какой документ является верхнеуровневым в иерархии ОРД организации и определяет общие цели, принципы и стратегию обеспечения информационной безопасности?
1. Инструкция по смене паролей.
2. Журнал учета электронных носителей.
3. Политика информационной безопасности.
4. Акт об уничтожении документов.</td><td>3</td></tr>
<tr><td>2</td><td>152.</td><td>Организационно-распорядительная документация по обеспечению информационной безопасности</td><td>При разработке проекта документа «Инструкция по антивирусной защите», какой раздел является обязательным для описания действий сотрудника при обнаружении признаков заражения ПК?
1. История создания антивирусного ПО.
2. Порядок действий при возникновении инцидента.
3. Технические характеристики процессора.
4. Список контактов поставщика оборудования.</td><td>2</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление соответствия (проверяет эксперт)</td></tr>
<tr><td>1</td><td>153.</td><td>Управление информационной безопасностью</td><td>Установите соответствие распорядительных документов и их целей в управлении ИБ<table><tr><td>Вид документа</td><td>Цель разработки документа</td></tr><tr><td>А) Приказ</td><td>1) Описание детального порядка действий при инцидентах</td></tr><tr><td>Б) Положение</td><td>2) Назначение ответственных лиц и ввод документов в действие</td></tr><tr><td>В) Регламент</td><td>3) Определение структуры и функций подразделения защиты</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>1</td><td>154.</td><td>Управление информационной безопасностью</td><td>Установите соответствие реквизитов документа ИБ и их назначения (по ГОСТ)<table><tr><td>Реквизит</td><td>Значение для управления документом</td></tr><tr><td>А) Гриф утверждения</td><td>1) Подтверждение согласия должностного лица с проектом</td></tr><tr><td>Б) Виза согласования</td><td>2) Придание документу официальной юридической силы</td></tr><tr><td>В) Гриф секретности</td><td>3) Определение правил обращения с носителем информации</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
<tr><td>2</td><td>155.</td><td>Организационно-распорядительная документация по обеспечению информационной безопасности</td><td>Установите соответствие категорий документов и их назначения<table><tr><td>Категория документа</td><td>Основное назначение в системе ИБ</td></tr><tr><td>А) Политика ИБ</td><td>1) Описание пошаговых действий сотрудника при возникновении инцидента</td></tr><tr><td>Б) Регламент</td><td>2) Определение общих целей, принципов и стратегию защиты информации</td></tr><tr><td>В) Инструкция</td><td>3) Описание порядка выполнения конкретного технологического процесса</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
<tr><td>2</td><td>156.</td><td>Организационно-распорядительная документация по обеспечению информационной безопасности</td><td>Установите соответствие документов по ИБ и их содержания<table><tr><td>Название документа</td><td>Ключевое содержание</td></tr><tr><td>А) Перечень ПДн</td><td>1) Правила использования сменных носителей информации</td></tr><tr><td>Б) Модель угроз</td><td>2) Список категорий данных, обрабатываемых в организации</td></tr><tr><td>В) Инструкция по антивирусной защите</td><td>3) Описание возможных каналов утечки и типов нарушителей</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление последовательности (проверяет эксперт)</td></tr>
<tr><td>1</td><td>157.</td><td>Управление информационной безопасностью</td><td>Расположите типы документов по информационной безопасности в порядке убывания их приоритетности в иерархии системы управления ИБ (СУИБ):</td><td>2, 3, 1, 4.</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			1. Регламент проведения антивирусных проверок. 2. Федеральное законодательство в области ИБ. 3. Политика информационной безопасности организации. 4. Должностная инструкция администратора ИБ.	
1	158.	Управление информационной безопасностью	Установите последовательность действий при подготовке проекта приказа о назначении ответственных за защиту персональных данных: 1. Визирование проекта приказа у юриста и начальника отдела кадров. 2. Определение круга должностных лиц, которые будут обрабатывать данные. 3. Регистрация подписанного приказа и присвоение ему номера. 4. Составление текста приказа с указанием конкретных обязанностей лиц.	2, 4, 1, 3.
2	159.	Организационно-распорядительная документация по обеспечению информационной безопасности	Установите правильную последовательность жизненного цикла локального нормативного акта по информационной безопасности: 1. Согласование проекта документа с заинтересованными подразделениями (ИТ, юристы, кадры). 2. Подготовка проекта текста документа ответственным исполнителем. 3. Ознакомление сотрудников организации с документом под роспись. 4. Утверждение документа приказом руководителя организации.	2, 1, 4, 3.
2	160.	Организационно-распорядительная документация по обеспечению информационной безопасности	Расположите типы документов по информационной безопасности в порядке убывания их юридической силы и иерархии в организации: 1. Инструкция администратора конкретной информационной системы. 2. Приказ руководителя о введении режима защиты информации. 3. Политика информационной безопасности организации. 4. Регламент взаимодействия при возникновении инцидентов ИБ.	3, 2, 4, 1.
Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)				
2	161.	Производственная, Проектно-технологическая практика	Кейс-задача: «Организация защищенного удаленного доступа к корпоративной сети». Руководство компании приняло решение перевести ИТ-отдел на удаленный режим работы. Вам, как специалисту по защите информации, поручено реализовать проект по обеспечению безопасности этого процесса. Задание: Подготовьте структуру краткого приказа о введении режима удаленной работы с точки зрения ИБ.	Документ должен включать: 1. Список сотрудников, допущенных к удаленной работе. 2. Обязанность сотрудников использовать только корпоративное ПО для связи. 3. Запрет на передачу учетных данных третьим лицам. 4. Ответственность за нарушение правил работы с конфиденциальной информацией.
2	162.	Производственная, Проектно-технологическая практика	Кейс-задача: «Внедрение системы защиты от утечек (DLP) в юридическом департаменте». В юридическом департаменте крупной компании участились случаи случайной пересылки конфиденциальных договоров на личные адреса сотрудников. Вам поручено проработать вопрос внедрения системы контроля	Необходимо разработать «Положение о порядке использования корпоративной электронной почты». Разделы: 1. Уведомление сотрудников о

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			почтового трафика. Задание: Какой локальный нормативный акт необходимо разработать, чтобы проверка почты сотрудников была законной? Перечислите 2 ключевых раздела этого документа.	том, что почта используется исключительно в рабочих целях и подлежит автоматизированному контролю. 2. Ответственность за попытки обхода средств защиты информации.
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
1	163.	Управление информационной безопасностью	Совокупность документов, регламентирующих вопросы защиты информации и изданных руководством организации в рамках своей компетенции, составляет организационно-_____ документацию по ИБ.	распорядительную
1	164.	Управление информационной безопасностью	При разработке проекта документа, устанавливающего запрет на разглашение коммерческой тайны, обязательным приложением к трудовому договору является _____ о неразглашении.	Обязательство
1	165.	Управление информационной безопасностью	Реквизит документа, содержащий дату, регистрационный номер и место составления, называется _____ данными документа.	справочными
1	166.	Управление информационной безопасностью	Документ, определяющий задачи, функции, права и ответственность подразделения (отдела), отвечающего за защиту информации в компании, называется _____ об отделе ИБ.	Положение
2	167.	Организационно-распорядительная документация по обеспечению информационной безопасности	Документ, определяющий высокоуровневые цели, принципы и общую стратегию защиты информации в организации, называется _____ информационной безопасности.	Политика
2	168.	Организационно-распорядительная документация по обеспечению информационной безопасности	Процедура предварительного рассмотрения и подтверждения согласия с содержанием проекта документа со стороны заинтересованных должностных лиц (юристов, ИТ-директора и др.) называется _____ документа.	Согласование (или Визирование)
2	169.	Организационно-распорядительная документация по	Локальный нормативный акт, детально описывающий порядок выполнения конкретных действий пользователем или администратором при работе со средствами защиты информации, называется _____.	Инструкция

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
		обеспечению информационной безопасности		
2	170.	Организационно-распорядительная документация по обеспечению информационной безопасности	Совокупность документов, определяющих порядок функционирования системы защиты информации и обязанности персонала, составляет _____ базу обеспечения информационной безопасности организации.	Нормативно-методическую (или Организационно-распорядительную).
Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных				
2	171.	Производственная, Проектно-технологическая практика	«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберете правильный ответ и объясните свой выбора. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2
2	172.	Производственная, Проектно-технологическая практика	«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании.	3

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	

ОПК-4 Способен осуществлять сбор, обработку и анализ научно-технической информации по теме исследования, разрабатывать планы и программы проведения научных исследований и технических разработок

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных				
1	173.	Основы научных исследований	Какая из перечисленных платформ является ведущей международной наукометрической базой данных? 1) Instagram 2) Scopus 3) Pinterest 4) LinkedIn	2
1	174.	Основы научных исследований	Какой формат файлов является стандартом для представления электронных постеров на международных конференциях? 1) .exe 2) .pdf 3) .mp3 4) .txt	2
Задание закрытого типа на установление соответствия (проверяет эксперт)				
1	175.	Основы научных исследований	Соотнесите этапы подготовки научного исследования с их описаниями: Этап — Описание A. Формулировка цели и задач исследования — 1. Поиск и систематизация научных данных и источников B. Сбор информации — 2. Создание графика и плана проведения исследований C. Разработка плана и программы — 3. Определение конкретных направлений и целей работы	A-3, B-1, C-2
1	176.	Основы научных исследований	Соотнесите результат исследования с его характеристикой: Результат — Описание	A-3, B-1, C-2

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td><table>
<tr><td>A. Научный отчет</td><td>1. Обобщение существующих данных по теме</td></tr>
<tr><td>B. Обзор литературы</td><td>2. Официальная публикация с исследовательскими данными</td></tr>
<tr><td>C. Научная статья</td><td>3. Документ с результатами, выводами и рекомендациями</td></tr>
</table></td><td></td></tr>
<tr><td colspan="5">Задание закрытого типа на установление последовательности (проверяет эксперт)</td></tr>
<tr><td>1</td><td>177.</td><td>Основы научных исследований</td><td>Расположите этапы подготовки научного исследования в правильной последовательности:
1. Формулировка гипотезы
2. Сбор и систематизация информации
3. Обработка и анализ данных
4. Постановка цели и задач исследования</td><td>4, 1, 2, 3</td></tr>
<tr><td>1</td><td>178.</td><td>Основы научных исследований</td><td>Расположите этапы сбора и анализа информации по порядку:
1. Оценка и отбор подходящих источников информации
2. Получение и фиксация данных
3. Обработка и систематизация полученной информации
4. Анализ и интерпретация данных для принятия решений</td><td>1, 2, 3, 4</td></tr>
<tr><td colspan="5">Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)</td></tr>
<tr><td>2</td><td>179.</td><td>Производственная, Проектно-технологическая практика</td><td>Кейс-задача: «Организация защищенного удаленного доступа к корпоративной сети». Руководство компании приняло решение перевести ИТ-отдел на удаленный режим работы. Вам, как специалисту по защите информации, поручено реализовать проект по обеспечению безопасности этого процесса.
Задание: Составьте план сравнительного анализа двух решений для VPN.</td><td>План включает: 1. Поиск документации и отзывов об уязвимостях обоих протоколов. 2. Сравнение поддерживаемых алгоритмов шифрования. 3. Анализ сложности настройки и поддержки. 4. Оценка производительности на основе технических обзоров.</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
2	180.	Производственная, Проектно-технологическая практика	Кейс-задача: «Внедрение системы защиты от утечек (DLP) в юридическом департаменте». В юридическом департаменте крупной компании участились случаи случайной пересылки конфиденциальных договоров на личные адреса сотрудников. Вам поручено проработать вопрос внедрения системы контроля почтового трафика. Задание: Составьте план поиска информации для выбора между «коробочным» DLP-решением и Open Source аналогом.	1. Изучение реестра отечественного ПО для подбора решений, соответствующих требованиям импортозамещения. 2. Анализ документации вендоров для оценки качества лингвистического анализа. 3. Сбор статистики по известным уязвимостям выбранных решений в базах БДУ ФСТЭК.
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
1	181.	Основы научных исследований	Что такое «Abstract» в структуре научной статьи на английском языке это _	резюме
1	182.	Основы научных исследований	Как называется процесс критической оценки научной работы экспертами в той же области перед её публикацией?	Рецензирование
Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных				
2	183.	Производственная, Проектно-технологическая практика	«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберете правильный ответ и объясните свой выбора. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2
2	184.	Производственная, Проектно-технологическая практика	«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как количество ошибок доступа (утечек) возросло. Необходимо выбрать	3

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	

ОПК-5 Способен проводить научные исследования, включая экспериментальные, обрабатывать результаты исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных				
1	185.	Основы научных исследований	Научно-технический потенциал включает: 1. организационно-управленческую структуру 2. научные кадры 3. материально-техническую базу 4. информационную составляющую 5. все ответы верны	5
1	186.	Основы научных исследований	Не пересекаются множества чисел: 1. простых и нечетных; 2. простых и четных; 3. простых и составных; 4. составных и нечетных.	3
Задание закрытого типа на установление соответствия (проверяет эксперт)				
1	187.	Основы научных исследований	Соотнесите тип документа с его содержанием: Документ — Содержание A. Научная статья — 1. Краткое изложение выполненной работы и выводов B. Научно-технический — 2. Презентация результатов перед	A-4, B-1, C-3, D-2

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><td>отчет</td><td>аудиторией</td></tr><tr><td>C. Обзор литературы</td><td>3. Обобщение существующих данных по теме исследование</td></tr><tr><td>D. Доклад на конференции</td><td>4. Детальное описание метода и результатов исследования</td></tr></table></td><td></td></tr>
<tr><td>1</td><td>188.</td><td>Основы научных исследований</td><td>Соотнесите виды исследований с их характеристиками:<table><tr><td>Вид исследования</td><td>Характеристика</td></tr><tr><td>A. Экспериментальные</td><td>1. Проведение опытов для подтверждения гипотезы</td></tr><tr><td>B. Теоретические</td><td>2. Разработка моделей и выводов на основе анализа литературы</td></tr></table></td><td>A – 1, B – 2</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление последовательности (проверяет эксперт)</td></tr>
<tr><td>1</td><td>189.</td><td>Основы научных исследований</td><td>Укажите порядок действий при подготовке научного доклада или статьи:
1. Анализ и интерпретация результатов исследования
2. Написание текста и оформление документа
3. Обзор литературы и подготовка плана
4. Представление и защита работы</td><td>3, 1, 2, 4</td></tr>
<tr><td>1</td><td>190.</td><td>Основы научных исследований</td><td>Укажите правильную последовательность действий при обработке и публикации результатов исследования:
1. Подготовка научного отчета или статьи
2. Проведение анализа и интерпретации данных
3. Представление результатов коллегам или на конференции
4. Сбор экспериментальных данных и их обработка</td><td>4, 2, 1, 3</td></tr>
<tr><td colspan="5">Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)</td></tr>
<tr><td>2</td><td>191.</td><td>Производственная, Проектно-технологическая практика</td><td>Кейс-задача: «Организация защищенного удаленного доступа к корпоративной сети». Руководство компании приняло решение перевести ИТ-отдел на удаленный режим работы. Вам, как специалисту по защите информации, поручено реализовать проект по обеспечению безопасности этого процесса.
Задание: Опишите методику эксперимента по проверке влияния VPN на скорость работы корпоративной CRM-системы.</td><td>1. Замерить время загрузки главной страницы без VPN (5 попыток). 2. Включить VPN и провести аналогичные замеры. 3. Вычислить среднее значение и процент задержки. 4. Оформить результат в виде краткого отчета с выводом: «Внедрение защиты замедляет работу системы на X%, что является допустимым в рамках</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
				требований бизнеса.
2	192.	Производственная, Проектно-технологическая практика	Кейс-задача: «Внедрение системы защиты от утечек (DLP) в юридическом департаменте». В юридическом департаменте крупной компании участились случаи случайной пересылки конфиденциальных договоров на личные адреса сотрудников. Вам поручено проработать вопрос внедрения системы контроля почтового трафика. Задание: Проведите эксперимент: проверьте, распознает ли система документ, если его заархивировать с паролем. Опишите результат в отчете.	○ Ход эксперимента: Отправка тестового письма с обычным файлом (контроль) и файла в запароленном архиве .zip. ○ Результат для отчета: Система заблокировала обычный файл, но пропустила архив, так как не смогла его вскрыть для анализа.
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
1	193.	Основы научных исследований	Преднамеренное, целенаправленное восприятие объекта, явления с целью изучения его свойств, особенностей протекания и поведения это _____	наблюдение
1	194.	Основы научных исследований	Метод познания, заключающийся в расчленение, разложение объекта исследования на составные части это _____.	анализ
Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных				
2	195.	Производственная, Проектно-технологическая практика	«Выбор и внедрение системы обнаружения вторжений (IDS/IPS)». Вам необходимо защитить периметр сети организации от сетевых атак. Руководство предлагает выбрать один из трех вариантов реализации системы обнаружения и предотвращения вторжений (IDS/IPS). Какое решение является наиболее полным и корректным с точки зрения проектирования системы ИБ в соответствии с государственными стандартами и требованиями регуляторов? Выберете правильный ответ и объясните свой выбора. Варианты ответа: 1. Установка бесплатной Open Source IDS Snort на старый офисный компьютер без оформления документации. 2. Закупка и внедрение программно-аппаратного комплекса (ПАК) класса IPS, имеющего действующий сертификат ФСТЭК России, с последующей разработкой ТЗ, Технического проекта и Инструкции администратора. 3. Написание собственного уникального алгоритма анализа трафика на языке Python и его запуск на сервере компании для проведения научного эксперимента без интеграции в общую систему защиты.	2
2	196.	Производственная, Проектно-технологическая практика	«Внедрение системы управления доступом». В компании используется файловый сервер с общими папками, доступ к которым выдается вручную администратором. В необходимо модернизировать этот процесс, так как	3

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			количество ошибок доступа (утечек) возросло. Необходимо выбрать стратегию действий. Какая последовательность действий является методологически верной для реализации полноценного цикла защиты информации? Варианты ответа: 1. Срочно запретить доступ всем сотрудникам к серверу и разрешать его только по личному звонку руководителю, не составляя никаких документов. 2. Написать научную статью о методах биометрической идентификации в будущем, не предлагая решения для текущей проблемы компании. 3. Проанализировать существующие угрозы, разработать проект ТЗ на внедрение системы централизованного управления доступом, спроектировать схему её интеграции в сеть, подготовить регламент парольной политики и провести тестирование системы на устойчивость к попыткам несанкционированного входа.	

ПК-1 Владеет методикой проведения предпроектного обследования объектов информатизации и выделенных(защищаемых) помещений

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных				
3	197.	Организация защиты объектов информатизации	Какая основная цель проведения предпроектного обследования объекта информатизации (ОИ)? 1. Закупка максимального количества средств защиты информации. 2. Сбор исходных данных о характеристиках объекта и выявление каналов утечки информации. 3. Обучение сотрудников правилам противопожарной безопасности. 4. Выбор поставщика офисной мебели для защищаемого помещения.	2
3	198.	Организация защиты объектов информатизации	Как называется помещение, предназначенное для проведения секретных переговоров, в котором исключено пребывание лиц без соответствующего допуска? 1. Санитарно-защитная зона. 2. Служебный кабинет. 3. Выделенное (защищаемое) помещение. 4. Помещение общего доступа.	3
3	199.	Организация защиты объектов информатизации	Что из перечисленного является первоочередным действием при обследовании «границ» защищаемого объекта?	2

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td>1. Проверка работоспособности принтеров.
2. Определение контролируемой зоны (КЗ) объекта.
3. Инвентаризация лицензий на антивирусное ПО.
4. Измерение температуры воздуха в серверной.</td><td></td></tr>
<tr><td>3</td><td>200.</td><td>Организация защиты объектов информатизации</td><td>Каким документом оформляются результаты проведенного предпроектного обследования объекта информатизации?
1. Приказ о назначении комиссии.
2. Акт обследования объекта.
3. Журнал учета посетителей.
4. Справка о стоимости оборудования.</td><td>2</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление соответствия (проверяет эксперт)</td></tr>
<tr><td>3</td><td>201.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие каналов утечки и физических сред распространения
<table><tr><td>Канал утечки</td><td>Среда распространения сигнала</td></tr><tr><td>А) Акустический</td><td>1) Остекление окон, стены, трубы отопления</td></tr><tr><td>Б) Виброакустический</td><td>2) Воздушное пространство внутри и вне помещения</td></tr><tr><td>В) Оптический</td><td>3) Прямая видимость (световые волны)</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
<tr><td>3</td><td>202.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие зон безопасности и их характеристик
<table><tr><td>Тип зоны</td><td>Характеристика в ходе обследования</td></tr><tr><td>А) Контролируемая зона</td><td>1) Территория, на которой исключено пребывание лиц без допуска</td></tr><tr><td>Б) Зона 1</td><td>2) Радиус, в котором возможно перехватить побочные излучения (ПЭМИН)</td></tr><tr><td>В) Санитарная зона</td><td>3) Территория вокруг объекта, свободная от застройки и ВТСС</td></tr></table></td><td>А - 1, Б - 2, В - 3.</td></tr>
<tr><td>3</td><td>203.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие методов обследования и их содержания
<table><tr><td>Метод обследования</td><td>Действие комиссии</td></tr><tr><td>А) Документальный</td><td>1) Визуальный осмотр конструкций, коммуникаций и розеток</td></tr><tr><td>Б) Визуальный</td><td>2) Измерение характеристик сигналов и зашумления</td></tr></table></td><td>А - 3, Б - 1, В - 2.</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><td>В) Инструментальный</td><td>3) Изучение планов БТИ, схем электропитания и заземления</td></tr></table></td><td></td></tr>
<tr><td>3</td><td>204.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие документов и этапов обследования<table><tr><td>Документ</td><td>Этап, на котором он создается</td></tr><tr><td>А) Приказ о создании комиссии</td><td>1) Завершение обследования</td></tr><tr><td>Б) Программа обследования</td><td>2) Подготовка к проведению работ</td></tr><tr><td>В) Акт обследования</td><td>3) Начало работ (организационный этап)</td></tr></table></td><td>А - 3, Б - 2, В - 1.</td></tr>
<tr><td>3</td><td>205.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие технических систем и потенциальных каналов утечки<table><tr><td>Система</td><td>Возможный канал утечки</td></tr><tr><td>А) Вентиляционные короба</td><td>1) Электромагнитные наводки в линиях питания</td></tr><tr><td>Б) Сеть электропитания</td><td>2) Акустический канал (передача звука через воздуховоды)</td></tr><tr><td>В) Система отопления</td><td>3) Виброакустический канал (вибрация труб)</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
<tr><td>3</td><td>206.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие реквизитов Акта обследования и их функций<table><tr><td>Реквизит</td><td>Значение для проекта защиты</td></tr><tr><td>А) Состав комиссии</td><td>1) Юридическое закрепление результатов обследования</td></tr><tr><td>Б) Заключение (выводы)</td><td>2) Определение круга лиц, несущих ответственность за аудит</td></tr><tr><td>В) Гриф секретности</td><td>3) Обоснование необходимости внедрения конкретных СЗИ</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление последовательности (проверяет эксперт)</td></tr>
<tr><td>3</td><td>207.</td><td>Организация защиты объектов информатизации</td><td>Установите хронологическую последовательность этапов предпроектного обследования объекта информатизации:</td><td>4, 2, 1, 3.</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			1. Визуальный осмотр помещений и инженерных систем. 2. Изучение технической документации и планов здания. 3. Оформление итогового Акта обследования с выводами. 4. Издание приказа о создании комиссии по обследованию.	
3	208.	Организация защиты объектов информатизации	Расставьте этапы выявления технических каналов утечки информации на объекте: 1. Проверка наличия и состояния звукоизоляции и экранирования. 2. Идентификация возможных физических сред распространения сигналов. 3. Оценка вероятности перехвата информации за границей зоны защиты. 4. Инструментальные измерения (при необходимости).	2, 1, 4, 3.
3	209.	Организация защиты объектов информатизации	Установите последовательность действий при обследовании границ контролируемой зоны: 1. Выявление наиболее критических точек (окон, дверей, вводов коммуникаций). 2. Определение фактической границы территории, охраняемой организацией. 3. Сопоставление фактической границы с расчетной зоной возможного перехвата. 4. Занесение границ контролируемой зоны на план-схему объекта.	2, 1, 3, 4.
3	210.	Организация защиты объектов информатизации	Установите порядок подготовки отчетной документации: 1. Формулирование рекомендаций по дооснащению объекта средствами защиты. 2. Описание текущего состояния защищенности объекта. 3. Подписание акта всеми членами комиссии. 4. Утверждение акта обследования руководителем организации.	2, 1, 3, 4.
Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)				
4	211.	Производственная, Преддипломная практика	Составьте перечень объектов обследования в выделенном помещении перед его аттестацией.	Определение границ контролируемой зоны, фиксация всех ОТСС и ВТСС(основные технические средства и системы вспомогательные технические средства и системы), проверка наличия инженерных коммуникаций, выходящих за пределы выделенного помещения.
4	212.	Производственная, Преддипломная практика	Проведите обследование ЛВС филиала для выявления неучтенных точек доступа.	Использование сетевых сканеров и визуальный осмотр коммутационных узлов. Итогом является актуализированная топология сети.

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
3	213.	Организация защиты объектов информатизации	Специально оборудованное помещение (кабинет, зал совещаний), предназначенное для проведения работ с конфиденциальной или секретной информацией, в нормативной документации называется _____ помещением.	выделенным (или защищаемым).
3	214.	Организация защиты объектов информатизации	Совокупность организационных и технических мер, реализуемых на объекте для предотвращения несанкционированного доступа посторонних лиц в пределы контролируемой зоны, составляет систему _____ безопасности.	физической
3	215.	Организация защиты объектов информатизации	В ходе предпроектного обследования изучение архитектурно-планировочных решений, схем электропитания и заземления объекта проводится в рамках _____ этапа работ.	документального (или ознакомительного)
3	216.	Организация защиты объектов информатизации	Нежелательные электромагнитные сигналы, возникающие при работе технических средств обработки информации и способные содержать защищаемые данные, называются побочными электромагнитными _____ и наводками.	излучениями (ПЭМИН).
3	217.	Организация защиты объектов информатизации	Проверка наличия у установленных на объекте средств защиты информации (фильтров, генераторов шума) действующих _____ соответствия является обязательной частью обследования.	сертификатов
3	218.	Организация защиты объектов информатизации	При обследовании объекта информатизации технический канал утечки, возникающий из-за преобразования звуковых колебаний в электрические сигналы в компонентах систем сигнализации или часофикации, называется _____.	акустоэлектрическим
Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора				
4	219.	Производственная, Преддипломная практика	«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования вы выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию?	2 Выполнение предпроектного обследования позволяет выявить канал утечки через смежную стену. На основе этого дается аналитическое обоснование необходимости СЗИ от НСД для выполнения требований регулятора.

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	
4	220.	Производственная, Преддипломная практика	При обследовании выделенного помещения (ВП) для совещаний за подвесным потолком обнаружен старый неиспользуемый громкоговоритель оповещения. Какое действие методически верно? 1. Оставить его, если он не подключен к проводам. 2. Зафиксировать как вспомогательное техническое средство и настоять на его демонтаже или защите фильтрами. 3. Использовать его для трансляции музыки, чтобы скрыть звуки переговоров. 4. Проверить, не спрятана ли в нем камера, и оставить на месте.	2. Методика обследования объектов информатизации требует выявления всех физических тел, способных создавать каналы утечки. Любое стороннее оборудование в ВП - это риск несанкционированного съема информации.

ПК-2 Способен приводить аналитическое обоснование необходимости создания систем защиты информации

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных				
3	221.	Организация защиты объектов информатизации	Текст задания: Какое аналитическое действие является первичным при обосновании необходимости создания системы защиты конкретного объекта информатизации? 1. Закупка сертифицированных генераторов шума. 2. Выявление потенциальных технических каналов утечки информации на объекте. 3. Назначение ответственного за противопожарную безопасность. 4. Окраска стен в защищаемом помещении в нейтральные цвета.	2
3	222.	Организация защиты объектов информатизации	Выберите факторы, которые служат аналитическим обоснованием для внедрения систем виброакустической защиты в выделенном помещении: (Выбор нескольких ответов) 1. Наличие инженерных коммуникаций (труб отопления), выходящих за пределы контролируемой зоны.	1, 3, 5.

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td>2. Использование в помещении только жидкокристаллических мониторов.
3. Расположение помещения на первом этаже с окнами, выходящими на общедоступную территорию.
4. Наличие в помещении вспомогательных технических средств (телефонов, датчиков сигнализации).
5. Недостаточная звукоизоляция ограждающих конструкций (стен, дверей).</td><td></td></tr>
<tr><td>3</td><td>223.</td><td>Организация защиты объектов информатизации</td><td>При обосновании проекта защиты, расчет радиуса зоны, в которой возможен перехват побочных электромагнитных излучений (ПЭМИН), проводится с целью:
1. Оценки стоимости электроэнергии.
2. Определения необходимых границ контролируемой зоны (КЗ).
3. Выбора модели системного блока.
4. Расчета освещенности рабочих мест.</td><td>2</td></tr>
<tr><td>3</td><td>224.</td><td>Организация защиты объектов информатизации</td><td>Какие сведения, полученные в ходе предпроектного анализа, обосновывают категорию объекта информатизации (1, 2 или 3)? (Выбор нескольких ответов)
1. Степень секретности или уровень конфиденциальности обрабатываемой информации.
2. Марка и модель используемых принтеров.
3. Масштаб возможного ущерба государству или организации при утечке данных.
4. Количество установленных в здании огнетушителей.</td><td>1, 3.</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление соответствия (проверяет эксперт)</td></tr>
<tr><td>3</td><td>225.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие выявленных угроз и проектных решений по их нейтрализации
<table><tr><th>Угроза (канал утечки)</th><th>Обоснованное проектное решение</th></tr><tr><td>А) Акустический (через щели в дверях)</td><td>1) Установка сетевых помехоподавляющих фильтров</td></tr><tr><td>Б) Электромагнитные наводки в сети питания</td><td>2) Использование виброакустических зашумляющих устройств</td></tr><tr><td>В) Виброакустический (через трубы отопления)</td><td>3) Уплотнение дверных притворов и установка тамбуров</td></tr></table></td><td>А - 3, Б - 1, В - 2.</td></tr>
<tr><td>3</td><td>226.</td><td>Организация защиты</td><td>Установите соответствие факторов риска и объектов аналитического</td><td>А - 3, Б - 1, В - 2.</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td>объектов информатизации</td><td>обследования<table><tr><td>Фактор риска</td><td>Объект анализа при обосновании</td></tr><tr><td>А) Просматриваемость окон с улицы</td><td>1) Стены, перекрытия и оконные блоки</td></tr><tr><td>Б) Недостаточная звукоизоляция</td><td>2) Инженерные коммуникации (вентиляция, трубы)</td></tr><tr><td>В) Наличие паразитных связей</td><td>3) Ландшафт и застройка вокруг объекта</td></tr></table></td><td></td></tr>
<tr><td>3</td><td>227.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие категорий объектов и критериев их присвоения<table><tr><td>Категория объекта</td><td>Критерий о основания (гриф информации)</td></tr><tr><td>А) 1 категория</td><td>1) Сведения, составляющие государственную тайну (СС)</td></tr><tr><td>Б) 2 категория</td><td>2) Сведения, составляющие государственную тайну (ОВ)</td></tr><tr><td>В) 3 категория</td><td>3) Сведения, составляющие государственную тайну (С)</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
<tr><td>3</td><td>228.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие физических полей и методов их инструментального анализа<table><tr><td>Физическое поле</td><td>Метод обоснования защищенности</td></tr><tr><td>А) Электромагнитное излучение</td><td>1) Измерение уровня звукового давления за грани ей ВП</td></tr><tr><td>Б) Акустическое поле</td><td>2) Измерение виброускорения на поверхностях конструкций</td></tr><tr><td>В) Вибрационное поле</td><td>3) Измерение напряженности поля на частотах работы ОТСС</td></tr></table></td><td>А - 3, Б - 1, В - 2.</td></tr>
<tr><td>3</td><td>229.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие типов технических средств и требований к их защите<table><tr><td>Тип средств</td><td>Обоснование необходимости защиты</td></tr><tr><td>А) ОТСС</td><td>1) Требуют защиты от наводок и «микрофонного эффекта»</td></tr><tr><td>Б) ВТСС</td><td>2) Требуют защиты от ПЭМИН (перехвата данных)</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><td>В) СЗИ</td><td>3) Требуют подтверждения эффективности (аттестации)</td></tr></table></td><td></td></tr>
<tr><td>3</td><td>230.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие зон защиты и условий их обеспечения<table><tr><td>Тип зоны</td><td>Условие, обосновывающее границы</td></tr><tr><td>А) Контролируемая зона (КЗ)</td><td>1) Место, где уровень опасного сигнала ниже уровня шумов</td></tr><tr><td>Б) Зона защиты</td><td>2) Расстояние до границы, доступной для посторонних лиц</td></tr><tr><td>В) Радиус ПЭМИН</td><td>3) Пространство, внутри которого установлены СЗИ</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление последовательности (проверяет эксперт)</td></tr>
<tr><td>3</td><td>231.</td><td>Организация защиты объектов информатизации</td><td>Установите правильную последовательность этапов аналитического обоснования необходимости создания системы защиты объекта информатизации:
1. Оценка величины возможного ущерба от реализации выявленных угроз.
2. Идентификация информационных активов и определение их категории (грифа).
3. Выявление потенциальных технических каналов утечки информации на объекте.
4. Формулирование вывода о необходимости внедрения конкретных видов СЗИ.</td><td>2, 3, 1, 4.</td></tr>
<tr><td>3</td><td>232.</td><td>Организация защиты объектов информатизации</td><td>Расположите действия эксперта в логическом порядке при обосновании границ контролируемой зоны (КЗ) объекта:
1. Расчет радиуса зоны возможного перехвата побочных излучений (ПЭМИН).
2. Анализ существующего режима охраны и физических границ территории.
3. Сопоставление расчетной зоны перехвата с фактической границей КЗ.
4. Выработка рекомендаций по расширению КЗ или установке средств зашумления.</td><td>2, 1, 3, 4.</td></tr>
<tr><td>3</td><td>233.</td><td>Организация защиты объектов информатизации</td><td>Установите последовательность шагов при анализе акустической защищенности выделенного помещения для обоснования установки СЗИ:
1. Проведение расчетов словесной разборчивости речи за пределами помещения.
2. Измерение уровней тестового звукового сигнала и естественного шума.</td><td>2, 1, 3, 4</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			3. Сравнение полученных показателей с нормативными требованиями ФСТЭК. 4. Обоснование выбора пассивных (изоляция) или активных (генераторы) мер защиты.	
3	234.	Организация защиты объектов информатизации	Расставьте этапы выбора сертифицированных СЗИ в процессе подготовки аналитического обоснования проекта: 1. Анализ рынка и реестров ФСТЭК/ФСБ на предмет наличия подходящих средств. 2. Определение требуемого класса (эшелона) защиты на основе категории объекта. 3. Сверка технических характеристик СЗИ с выявленными параметрами каналов утечки. 4. Включение выбранных моделей средств защиты в итоговое обоснование (акт/проект).	2, 1, 3, 4.
Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)				
4	235.	Производственная, Преддипломная практика	Обоснуйте выбор между программным и аппаратно-программным модулем доверенной загрузки.	Сравнение по уровню контроля целостности: АПМДЗ блокирует доступ до загрузки ОС, что критично для защиты от подмены загрузчика.
4	236.	Производственная, Преддипломная практика	Приведите обоснование установки межсетевого экрана нового поколения.	Анализ статистики атак прикладного уровня, которые не видит обычный L3-firewall.
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
3	237.	Организация защиты объектов информатизации	Процесс выявления технических каналов утечки и оценки вероятности перехвата информации на объекте, служащий фундаментом для разработки системы защиты, называется аналитическим _____.	обоснованием
3	238.	Организация защиты объектов информатизации	При обосновании защиты выделенного помещения показатель, отражающий отношение уровня информативного акустического сигнала к уровню естественного шума, называется энергетическим _____ защищенности.	критерием
3	239.	Организация защиты объектов информатизации	Физическое лицо или техническое устройство, способное осуществить перехват информации за пределами контролируемой зоны объекта, классифицируется в аналитическом отчете как _____.	нарушитель
3	240.	Организация защиты объектов информатизации	Мера защиты, заключающаяся в использовании специальных экранов, фильтров и звукоизоляционных материалов для предотвращения выхода	пассивной

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			сигналов за границы объекта, называется _____ защитой.	
3	241.	Организация защиты объектов информатизации	Паразитную связь между цепями электропитания и линиями передачи данных, позволяющую перехватить информацию через розетки или трубы, в рамках обоснования проекта называют _____ наводками.	электромагнитными
3	242.	Организация защиты объектов информатизации	Документ, содержащий сведения о категории объекта и перечень всех актуальных технических каналов утечки, которые необходимо нейтрализовать, - это _____ по результатам обследования.	заключение (или акт).
Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора				
4	243.	Производственная, Преддипломная практика	«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования вы выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Выполнение предпроектного обследования позволяет выявить канал утечки через смежную стену. На основе этого дается аналитическое обоснование необходимости активной защиты.
4	244.	Производственная, Преддипломная практика	Руководство считает установку системы виброакустического зашумления окон избыточной тратой средств. Какое обоснование будет наиболее убедительным? 1. Это требование моды в современных офисах. 2. Анализ угроз подтверждает наличие риска дистанционного съема речи лазерным методом через оконные стекла. 3. Система зашумления также защищает от шума машин с улицы. 4. Стоимость системы невелика по сравнению с общим бюджетом.	2. Аналитическое обоснование базируется на сопоставлении модели угроз и конкретных мер защиты. Если канал утечки существует физически, его нейтрализация становится технологической необходимостью, а не опцией.

ПК-3 Владеет нормативно-методической базой обеспечения защиты сведений, составляющих государственную тайну

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td colspan="5">Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных</td></tr>
<tr><td>3</td><td>245.</td><td>Государственная тайна и защита информации</td><td>Какой федеральный закон является основным нормативным актом, регулирующим отношения в сфере защиты государственной тайны в РФ?
1. Федеральный закон «Об информации, информационных технологиях и о защите информации».
2. Закон РФ «О государственной тайне».
3. Федеральный закон «О безопасности».
4. Уголовный кодекс РФ.</td><td>2</td></tr>
<tr><td>3</td><td>246.</td><td>Государственная тайна и защита информации</td><td>Какая форма допуска оформляется гражданам для работы со сведениями, имеющими гриф «Совершенно секретно»?
1. Первая форма.
2. Вторая форма.
3. Третья форма.
4. Четвертая форма.</td><td>2</td></tr>
<tr><td>3</td><td>247.</td><td>Государственная тайна и защита информации</td><td>Кто несет персональную ответственность за организацию защиты сведений, составляющих государственную тайну, в организации?
1. Руководитель режимно-секретного подразделения.
2. Системный администратор.
3. Руководитель организации.
4. Начальник отдела кадров.</td><td>3</td></tr>
<tr><td>3</td><td>248.</td><td>Государственная тайна и защита информации</td><td>Какой орган исполнительной власти осуществляет лицензирование деятельности предприятий по проведению работ с использованием сведений, составляющих государственную тайну?
1. МВД России.
2. ФСБ России.
3. Роскомнадзор.
4. Министерство цифрового развития.</td><td>2</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление соответствия (проверяет эксперт)</td></tr>
<tr><td>3</td><td>249.</td><td>Государственная тайна и защита информации</td><td>Укажите соответствие форм допуска и категорий секретности
<table><tr><td>Форма допуска</td><td>Доступ к сведениям</td></tr><tr><td>А) Первая форма</td><td>1) К сведениям с грифом «Совершенно секретно»</td></tr><tr><td>Б) Вторая форма</td><td>2) К сведениям с грифом «Секретно»</td></tr><tr><td>В) Третья форма</td><td>3) К сведениям с грифом «Особой важности»</td></tr></table></td><td>А - 3, Б - 1, В - 2.</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td>3</td><td>250.</td><td>Государственная тайна и защита информации</td><td>Укажите соответствие органов защиты и их функций
<table><tr><td>Орган защиты</td><td>Основная задача</td></tr><tr><td>А) ФСБ России</td><td>1) Технический контроль и противодействие техническим разведкам</td></tr><tr><td>Б) ФСТЭК России</td><td>2) Контрразведывательное обеспечение и лицензирование работ с ГТ</td></tr><tr><td>В) Служба внешней разведки</td><td>3) Защита ГТ в загранучреждениях РФ</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
<tr><td>3</td><td>251.</td><td>Государственная тайна и защита информации</td><td>Укажите соответствие видов ответственности за нарушения в области ГТ
<table><tr><td>Вид ответственности</td><td>Пример правонарушения</td></tr><tr><td>А) Уголовная</td><td>1) Нарушение правил секретного делопроизводства без признаков шпионажа</td></tr><tr><td>Б) Административная</td><td>2) Государственная измена или разглашение ГТ с тяжкими последствиями</td></tr><tr><td>В) Дисциплинарная</td><td>3) Утрата секретного документа, не повлекшая тяжких последствий (по уставу)</td></tr></table></td><td>А - 2, Б -1, В - 3.</td></tr>
<tr><td>3</td><td>252.</td><td>Государственная тайна и защита информации</td><td>Укажите соответствие реквизитов на секретном носителе
<table><tr><td>Реквизит</td><td>Описание</td></tr><tr><td>А) Гриф секретности</td><td>1) Порядковый номер документа в журнале учета</td></tr><tr><td>Б) Регистрационный номер</td><td>2) Указание на должностное лицо, установившее секретность</td></tr><tr><td>В) Пункт Перечня</td><td>3) Степень секретности (ОВ, СС или С)</td></tr></table></td><td>А - 3, Б - 1, В - 2.</td></tr>
<tr><td>3</td><td>253.</td><td>Государственная тайна и защита информации</td><td>Укажите соответствие полномочий должностных лиц
<table><tr><td>Субъект</td><td>Полномочия в области ГТ</td></tr><tr><td>А) Президент РФ</td><td>1) Издает постановления по вопросам организации защиты ГТ</td></tr><tr><td>Б) Правительство РФ</td><td>2) Утверждает Государственную программу обеспечения защиты ГТ</td></tr><tr><td>В) Руководитель организации</td><td>3) Несет персональную ответственность</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><td></td><td>за режим в организации</td></tr></table></td><td></td></tr>
<tr><td>3</td><td>254.</td><td>Государственная тайна и защита информации</td><td>Укажите соответствие терминов и понятий<table><tr><td>Термин</td><td>Определение</td></tr><tr><td>А) Носители ГТ</td><td>1) Материальные объекты (предметы, файлы), в которых сведения отражены</td></tr><tr><td>Б) Система защиты ГТ</td><td>2) Органы защиты, используемые ими средства и методы</td></tr><tr><td>В) Перечень сведений</td><td>3) Документ, определяющий совокупность секретной информации</td></tr></table></td><td>А - 1, Б - 2, В - 3.</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление последовательности (проверяет эксперт)</td></tr>
<tr><td>3</td><td>255.</td><td>Государственная тайна и защита информации</td><td>Расположите грифы секретности в порядке убывания степени секретности сведений, которые они обозначают:
1. Совершенно секретно.
2. Секретно.
3 . Особой важности.</td><td>3, 1, 2.</td></tr>
<tr><td>3</td><td>256.</td><td>Государственная тайна и защита информации</td><td>Установите правильную последовательность этапов
процедуры засекречивания сведений:
1. Присвоение сведениям соответствующего грифа секретности.
2. Определение принадлежности сведений к Перечню, действующему в данном органе/организации.
3. Нанесение необходимых реквизитов на носитель информации.
4. Включение сведений в проект документа или на носитель.</td><td>2, 4, 1, 3.</td></tr>
<tr><td>3</td><td>257.</td><td>Государственная тайна и защита информации</td><td>Расположите формы допуска граждан к государственной тайне в порядке возрастания их значимости и строгости проверочных мероприятий (от низшей к высшей):
1. Вторая форма.
2. Третья форма.
3. Первая форма.</td><td>2, 1, 3.</td></tr>
<tr><td>3</td><td>258.</td><td>Государственная тайна и защита информации</td><td>Расставьте этапы оформления допуска гражданина к государственной тайне в хронологическом порядке:
1. Ознакомление гражданина с нормами законодательства о гостайне и обязательствами перед государством.
2. Письменное оформление согласия гражданина на частичные временные</td><td>1, 2, 4, 3.</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			ограничения его прав. 3. Принятие решения руководителем о допуске и издание соответствующего приказа (распоряжения). 4. Проведение проверочных мероприятий органами безопасности (для 1 и 2 форм).	
Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)				
3	259.	Производственная, Организационно-управленческая практика	В ходе аудита архива защищенного подразделения вы обнаружили неучтенный жесткий диск, на котором, по словам сотрудника, хранятся старые копии секретных документов. На диске нет никаких маркировок. Опишите ваши действия.	− Немедленно изъять носитель и изолировать его от любых вычислительных сетей. − Доложить руководству подразделения по защите государственной тайны. − Провести служебное расследование. − Принять решение о его уничтожении или официальном вводе в эксплуатацию.
3	260.	Производственная, Организационно-управленческая практика	В ходе аудита архива защищенного подразделения вы обнаружили неучтенный ноутбук, на котором, по словам сотрудника, хранятся старые файлы секретных документов. На ноутбуке нет никаких маркировок. Опишите ваши действия.	− Немедленная локализация и физическая защита − Документирование и информирование − Служебное расследование − Принятие итогового решения
4	261.	Производственная, Преддипломная практика	Укажите требования к хранению секретных носителей информации в нерабочее время.	Согласно нормам СТР, носители должны храниться в опечатываемых сейфах в специально оборудованных помещениях.
4	262.	Производственная, Преддипломная практика	Опишите порядок маркировки системного блока, предназначенного для обработки секретных сведений.	Нанесение бирки с инвентарным номером, грифом секретности и подписью ответственного за эксплуатацию.
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
3	263.	Государственная тайна и защита информации	Как называется процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий - на проведение работ с использованием таких сведений?	Допуск
3	264.	Государственная тайна и защита информации	Реквизиты, проставляемые на носителе сведений и (или) в сопроводительной документации на него, свидетельствующие о степени секретности сведений, называются _____ секретности.	Гриф (или Грифы).
3	265.	Государственная тайна и	Перенос сведений, составляющих государственную тайну, на носитель	Засекречивание

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
		защита информации	(бумажный, магнитный и др.) с присвоением соответствующего грифа секретности называется _____ сведений.	
3	266.	Государственная тайна и защита информации	Как называется высшая степень секретности сведений, составляющих государственную тайну?	Особой важности
3	267.	Государственная тайна и защита информации	Срок засекречивания сведений, составляющих государственную тайну, по общему правилу не должен превышать _____ лет.	30 (Тридцать).
3	268.	Государственная тайна и защита информации	Как называется документ, подтверждающий право учреждения или организации на осуществление деятельности, связанной с использованием сведений, составляющих государственную тайну?	Лицензия
Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора				
3	269.	Производственная, Организационно-управленческая практика	В ходе проверки архива в режимно-секретном подразделении (РСП) вы обнаружили флеш-накопитель с грифом «Секретно», лежащий на обычном рабочем столе в конце рабочего дня. Что требуют нормы СТР и Инструкции № 3-1? 1. Оставить флешку на месте, так как посторонних в помещении нет. 2. Немедленно изъять флеш-накопитель, поместить его в опечатываемый сейф и доложить руководству РСП о нарушении режима секретности. 3. Забрать флешку себе домой, чтобы она точно не пропала. 4. Положить флешку в карман и утром незаметно вернуть владельцу.	2 Нормативная база жестко регламентирует хранение носителей сведений, составляющих гостайну. В нерабочее время они обязаны находиться исключительно в опечатываемых сейфах спец. хранилищ.
3	270.	Производственная, Организационно-управленческая практика	Сотрудник просит скопировать файл с грифом «Секретно» на свой личный смартфон, чтобы поработать с документом дома. Каков ваш ответ на основе требований регуляторов? 1. Разрешить, если он пообещает никому не показывать этот файл. 2. Разрешить, если предварительно зашифровать файл паролем. 3. Категорически запретить, так как обработка секретных сведений на неаттестованных личных устройствах и их вынос за пределы контролируемой зоны запрещены. 4. Разрешить только в том случае, если на смартфоне установлен антивирус.	3 Защита гостайны строится на изоляции информации внутри аттестованного периметра. Вынос информации на неконтролируемые устройства образует критический канал утечки.
4	271.	Производственная, Преддипломная практика	«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования вы выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию?	2 Разработка документов ведется строго по нормативно-методической базе, что обязательно для объектов, связанных с государственной тайной.

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	
4	272.	Производственная, Преддипломная практика	Какое требование является обязательным при транспортировке жесткого диска со сведениями «секретно» между двумя зданиями организации? 1. Упаковка диска в пузырчатую пленку для защиты от ударов. 2. Помещение диска в опечатываемый спецпортфель (пенал) и передача через секретное подразделение с записью в журнале. 3. Сопровождение диска двумя охранниками с оружием. 4. Пересылка диска через обычную курьерскую службу.	2. Работа с гостайной регламентируется жесткой нормативной базой (Инструкция №3-1), которая определяет порядок учета и перемещения носителей только через уполномоченных лиц в защищенной таре.

ПК-4 Способен организовывать и сопровождать аттестацию объектов вычислительной техники и выделенных (защищаемых) помещений на соответствие требованиям по защите информации

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных				
3	273.	Организация защиты объектов информатизации	Какой документ является официальным разрешением на эксплуатацию объекта информатизации (ОИ) для обработки конфиденциальной информации или сведений, составляющих государственную тайну? 1. Лицензия ФСБ. 2. Программа и методика испытаний. 3. Аттестат соответствия. 4. Технический паспорт объекта.	3
3	274.	Организация защиты объектов информатизации	Выберите организации (субъекты), которые имеют право проводить аттестационные испытания объектов информатизации по требованиям защиты информации: (Выбор нескольких ответов) 1. Органы по аттестации (организации-лицензиаты ФСТЭК/ФСБ). 2. Отделы клининга и технического обслуживания зданий.	1, 3, 5.

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td>3. Государственные органы-регуляторы (ФСТЭК, ФСБ) в рамках контроля.
4. Любые IT-компании, занимающиеся продажей компьютеров.
5. Подразделения по защите информации самого предприятия (при наличии соответствующей лицензии).</td><td></td></tr>
<tr><td>3</td><td>275.</td><td>Организация защиты объектов информатизации</td><td>На какой максимальный срок обычно выдается Аттестат соответствия для объекта информатизации (при условии неизменности условий эксплуатации и архитектуры системы)?
1. На 1 год.
2. На 3 года (или 5 лет в зависимости от типа системы и нормативной базы).
3. Бессрочно.
4. До первой вирусной атаки.</td><td>2</td></tr>
<tr><td>3</td><td>276.</td><td>Организация защиты объектов информатизации</td><td>Какие действия входят в процедуру сопровождения аттестованного объекта в течение срока действия аттестата? (Выбор нескольких ответов)
1. Ежегодный контроль эффективности принятых мер защиты (контрольные проверки).
2. Смена интерьера и перестановка мебели без уведомления органа по аттестации.
3. Информирование органа по аттестации о существенных изменениях в составе ОТСС и ВТСС.
4. Ведение журналов учета СЗИ и периодическая проверка их работоспособности.</td><td>1, 3, 4.</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление соответствия (проверяет эксперт)</td></tr>
<tr><td>3</td><td>277.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие категорий объектов и проверяемых каналов утечки
<table><tr><td>Объект аттестации</td><td>Основной проверяемый канал утечки</td></tr><tr><td>А) Выделенное помещение (ВП)</td><td>1) Утечка через побочные электромагнитные излучения (ПЭМИН)</td></tr><tr><td>Б) Объект вычислительной техники (ОВТ)</td><td>2) Несанкционированный доступ (НСД) к информации</td></tr><tr><td>В) Информационная система (ИС)</td><td>3) Акустический и виброакустический каналы</td></tr></table></td><td>А - 3, Б - 1, В - 2.</td></tr>
<tr><td>3</td><td>278.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие документов аттестационного дела и их функций
<table><tr><td>Документ</td><td>Роль в процессе аттестации</td></tr><tr><td>А) Технический паспорт</td><td>1) Описание фактических результатов измерений и тестов</td></tr><tr><td>Б) Протокол испытаний</td><td>2) Подробная характеристика состава и</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td></td><td><table><tr><td></td><td>границ объекта</td></tr><tr><td>В) Аттестат соответствия</td><td>3) Официальное разрешение на обработку информации</td></tr></table></td><td></td></tr>
<tr><td>3</td><td>279.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие типов СЗИ и требований к их наличию в проекте<table><tr><td>Тип средства защиты</td><td>Требование при аттестации</td></tr><tr><td>А) Сертифицированные СЗИ</td><td>1) Должны быть установлены на все ВТСС</td></tr><tr><td>Б) Средства активной защиты</td><td>2) Обязательны для применения на аттестуемых объектах</td></tr><tr><td>В) Помехоподавляющие фильтры</td><td>3) Применяются, если пассивные меры недостаточно эффективны</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
<tr><td>3</td><td>280.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие видов контроля и их периодичности<table><tr><td>Вид контроля аттестованного объекта</td><td>Срок (частота) проведения</td></tr><tr><td>А) Первичная аттестация</td><td>1) Не реже одного раза в год</td></tr><tr><td>Б) Ежегодный контроль (мониторинг)</td><td>2) Проводится до начала обработки защищаемых данных</td></tr><tr><td>В) Переаттестация</td><td>3) Каждые 3 года или 5 лет (по истечении срока аттестата)</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
<tr><td>3</td><td>281.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие нарушений и последствий для аттестата<table><tr><td>Действие на объекте</td><td>Последствие для аттестата соответствия</td></tr><tr><td>А) Замена системного блока ОТСС</td><td>1) Сохранение действия аттестата без изменений</td></tr><tr><td>Б) Проведение плановой уборки</td><td>2) Приостановление действия или переаттестация</td></tr><tr><td>В) Перенос границ контролируемой зоны</td><td>3) Необходимость внесения изменений в техпаспорт и уведомления</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td>3</td><td>282.</td><td>Организация защиты объектов информатизации</td><td>Установите соответствие процедур и ответственных лиц<table><tr><td>Процедура</td><td>Ответственный исполнитель</td></tr><tr><td>А) Подача заявки на аттестацию</td><td>1) Регулятор (ФСТЭК / ФСБ)</td></tr><tr><td>Б) Проведение испытаний</td><td>2) Организация-владелец объекта (Заявитель)</td></tr><tr><td>В) Государственный надзор</td><td>3) Орган по аттестации (Лицензиат)</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление последовательности (проверяет эксперт)</td></tr>
<tr><td>3</td><td>283.</td><td>Организация защиты объектов информатизации</td><td>Установите правильную последовательность этапов проведения аттестации объекта информатизации (от подачи заявки до эксплуатации):
1. Проведение аттестационных испытаний (инструментальный контроль, анализ документации).
2. Подача заявки владельцем объекта в орган по аттестации (лицензиату ФСТЭК/ФСБ).
3. Оформление протоколов испытаний и выдача «Аттестата соответствия».
4. Предпроектное обследование и подготовка объекта к аттестации (установка СЗИ).</td><td>4, 2, 1, 3.</td></tr>
<tr><td>3</td><td>284.</td><td>Организация защиты объектов информатизации</td><td>Расположите действия в логическом порядке при осуществлении ежегодного контроля аттестованного объекта:
1. Проведение контрольных измерений характеристик побочных излучений и наводок.
2. Проверка неизменности состава технических средств (ОТСС и ВТСС) по техпаспорту.
3. Анализ журналов учета СЗИ и событий безопасности за прошедший год.
4. Оформление заключения о подтверждении действия аттестата соответствия.</td><td>2, 3, 1, 4.</td></tr>
<tr><td>3</td><td>285.</td><td>Организация защиты объектов информатизации</td><td>Установите последовательность действий при модернизации аттестованного объекта (например, замена сервера или АРМ):
1. Уведомление органа по аттестации о планируемых изменениях в системе.
2. Проведение дополнительных испытаний (контрольных проверок) новых компонентов.
3. Внесение изменений в технический паспорт объекта информатизации.
4. Принятие решения о продлении или переоформлении аттестата.</td><td>1, 3, 2, 4.</td></tr>
<tr><td>3</td><td>286.</td><td>Организация защиты объектов информатизации</td><td>Расставьте шаги по подготовке аттестационного дела (комплекта документов) на выделенное помещение:
1. Описание границ контролируемой зоны и расположения коммуникаций.</td><td>1, 2, 3, 4.</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			2. Составление перечня установленных средств защиты (генераторов шума, фильтров). 3. Сбор сертификатов соответствия на все используемые средства защиты информации. 4. Утверждение инструкции по порядку эксплуатации и режима секретности в помещении.	
Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)				
4	287.	Производственная, Организационно-управленческая практика	В ходе организационного этапа подготовки к аттестации выделенного помещения (для обсуждения сведений, составляющих государственную тайну) вы обнаружили, что в техническом паспорте на помещение отсутствует схема расположения основных и вспомогательных технических средств (ОТСС и ВТСС), а также не указаны границы контролируемой зоны. Опишите ваши действия как организатора и сопровождающего лица для устранения этой проблемы до приезда аттестационной комиссии.	1. Провести физический осмотр помещения и нанести на масштабную схему все установленные технические средства. 2. Определить и измерить расстояние от технических средств до границ контролируемой зоны. 3. Оформить полученные данные в виде графического приложения к техническому паспорту и утвердить обновленный техпаспорт у руководства предприятия.
4	288.	Производственная, Организационно-управленческая практика	В ходе организационного этапа подготовки к аттестации выделенного помещения (для обсуждения сведений, составляющих государственную тайну) вы обнаружили, что в техническом паспорте на помещение отсутствует схема расположения основных и вспомогательных технических средств (ОТСС и ВТСС), а также не указаны границы контролируемой зоны. Проведите анализ ситуации.	Эксплуатация и аттестация объекта без актуального и полного технического паспорта невозможна согласно требованиям нормативно-методических документов ФСТЭК России.
4	289.	Производственная, Преддипломная практика	Подготовьте проект программы и методики испытаний (ПМИ) автоматизированной системы.	Определение перечня проверок (парольная политика, антивирус, контроль целостности) и критериев успешности.
4	290.	Производственная, Преддипломная практика	Какие действия необходимо предпринять при обнаружении несоответствия настройки СЗИ требованиям аттестата в ходе проверки?	Приостановка работ, корректировка настроек согласно ТЗ и повторное сканирование уязвимостей.
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
3	291.	Организация защиты объектов информатизации	Текст задания: Официальный документ, подтверждающий, что объект информатизации соответствует требованиям стандартов и нормативных документов по безопасности информации, называется _____ соответствия.	аттестат

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
3	292.	Организация защиты объектов информатизации	Процедура проверки эффективности принятых мер защиты на аттестованном объекте, проводимая не реже одного раза в год в течение срока действия аттестата, называется ежегодным _____.	контролем (или мониторингом).
3	293.	Организация защиты объектов информатизации	Документ, содержащий подробные сведения о составе технических средств (ОТСС и ВТСС), границах контролируемой зоны и схемах электропитания объекта, называется технический _____.	паспорт
3	294.	Организация защиты объектов информатизации	Организация, обладающая лицензией ФСТЭК или ФСБ на право проведения работ по аттестации объектов информатизации, называется _____ по аттестации.	орган
3	295.	Организация защиты объектов информатизации	Документ, в котором фиксируются фактические результаты инструментальных измерений (например, уровней ПЭМИН или звукоизоляции) в ходе аттестационных испытаний, называется _____ испытаний.	протокол
3	296.	Организация защиты объектов информатизации	Срок действия аттестата соответствия для информационных систем, как правило, составляет от 3 до _____ лет (в зависимости от категории и типа системы).	5 (пяти).
Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора				
4	297.	Производственная, Организационно-управленческая практика	При сопровождении аттестации АС выяснилось, что на поставляемые серверы отсутствуют формуляры и сертификаты соответствия ФСТЭК России. Ваши действия? 1. Попросить аттестационную комиссию поверить вам на слово. 2. Приостановить процедуру аттестации и официально затребовать у поставщика или производителя недостающие формуляры и копии действующих сертификатов. 3. Скачать похожие сертификаты из Интернета и вставить туда названия своих серверов. 4. Сказать, что для внутренней сети сертификаты не нужны.	2 Сопровождение аттестации требует обеспечения легитимности всех СЗИ и средств обработки информации. Отсутствие обязательных документов делает аттестацию невозможной.
4	298.	Производственная, Организационно-управленческая практика	Орган по аттестации в ходе испытаний выявил, что длина паролей пользователей в системе составляет всего 4 символа (вместо 8 по ТЗ). Как должен поступить сопровождающий? 1. Доказывать комиссии, что 4 символа — это очень удобно для сотрудников.	3 Задача сопровождающего — содействовать успешному прохождению аттестации путем

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			2. Изменить текст ТЗ прямо во время проверки, снизив планку до 4 символов. 3. Признать несоответствие, оперативно перенастроить парольную политику на сервере до требуемых 8 символов и продемонстрировать исправление комиссии. 4. Предложить комиссии взятку за игнорирование этого пункта.	оперативного устранения выявленных недочетов, если они носят конфигурационный характер.
4	299.	Производственная, Преддипломная практика	«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования вы выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Только после выполнения всех технических и организационных мер объект готов к аттестации.
4	300.	Производственная, Преддипломная практика	В ходе аттестационных испытаний выяснилось, что на сервере не обновлены антивирусные базы. Ваши действия в роли сопровождающего? 1. Сообщить комиссии, что интернет временно не работает. 2. Признать несоответствие, немедленно обновить базы и предоставить отчет комиссии для фиксации в протоколе. 3. Предложить комиссии прийти на следующей неделе. 4. Удалить антивирус, чтобы он не мешал проверке.	2. Сопровождение аттестации подразумевает оперативное взаимодействие с экспертами и устранение мелких недостатков в ходе испытаний для получения «Аттестата соответствия» в срок.

ПК-5 Способен организовывать и проводить приемочные испытания СЗИ, вводить в эксплуатацию СЗИ

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных				

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
3	301.	Ввод системы защиты информации в эксплуатацию	На основании какого документа принимается окончательное решение о возможности эксплуатации системы защиты информации (СЗИ) в составе автоматизированной системы после успешного завершения всех этапов испытаний? 1. Журнал учета инцидентов. 2. Акт о приемке системы в эксплуатацию. 3. Техническое задание. 4. Должностная инструкция администратора.	2
3	302.	Ввод системы защиты информации в эксплуатацию	Какой документ определяет конкретный перечень проверок, методов и условий проведения испытаний СЗИ для подтверждения их соответствия техническому заданию? 1. Пояснительная записка. 2. Программа и методика испытаний (ПМИ). 3. Спецификация оборудования. 4. Формуляр на изделие.	2
3	303.	Организация приемочных испытаний системы защиты информации	Кто, как правило, возглавляет приемочную комиссию при организации испытаний системы защиты информации в организации? 1. Представитель компании-поставщика СЗИ. 2. Самый младший по должности сотрудник отдела ИТ. 3. Председатель комиссии (обычно руководитель организации или его заместитель). 4. Сторонний системный интегратор, не участвовавший в проекте.	3
3	304.	Организация приемочных испытаний системы защиты информации	Что должна сделать приемочная комиссия, если в ходе испытаний выявлены критические несоответствия СЗИ требованиям технического задания? 1. Игнорировать их и подписать акт приемки «как есть». 2. Самостоятельно переписать программный код системы. 3. Отразить недостатки в протоколе и направить систему на доработку. 4. Удалить техническое задание и составить новое под текущие функции.	3
Задание закрытого типа на установление соответствия (проверяет эксперт)				

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td>3</td><td>305.</td><td>Ввод системы защиты информации в эксплуатацию</td><td>Установите соответствие видов испытаний СЗИ и их целей<table><tr><td>Вид испытаний</td><td>Цель проведения в проекте</td></tr><tr><td>А) Предварительные испытания</td><td>1) Проверка готовности СЗИ к промышленной эксплуатации и принятие решения о вводе</td></tr><tr><td>Б) Опытная эксплуатация</td><td>2) Проверка работоспособности СЗИ и устранение выявленных недоработок</td></tr><tr><td>В) Приемочные испытания</td><td>3) Проверка СЗИ в условиях реальной работы персоналом организации</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
<tr><td>3</td><td>306.</td><td>Ввод системы защиты информации в эксплуатацию</td><td>Установите соответствие программных и методических документов их содержанию<table><tr><td>Документ</td><td>Содержит информацию о...</td></tr><tr><td>А) Программа испытаний</td><td>1) Конкретных действиях (шагах) по проверке каждой функции защиты</td></tr><tr><td>Б) Методика испытаний</td><td>2) Перечне объектов, сроках и условиях проведения проверок</td></tr><tr><td>В) Протокол испытаний</td><td>3) Фактических результатах проверок и выявленных несоответствиях</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
<tr><td>3</td><td>307.</td><td>Организация приемочных испытаний системы защиты информации</td><td>Установите соответствие этапов испытаний и их ключевых задач<table><tr><td>Этап испытаний</td><td>Основная задача</td></tr><tr><td>А) Предварительные испытания</td><td>1) Оценка готовности системы к постоянной эксплуатации и подписание акта</td></tr><tr><td>Б) Опытная эксплуатация</td><td>2) Проверка работоспособности СЗИ и устранение недоработок разработчиком</td></tr><tr><td>В) Приемочные испытания</td><td>3) Отработка навыков персонала и проверка стабильности СЗИ в реальных условиях</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
<tr><td>3</td><td>308.</td><td>Организация приемочных</td><td>Установите соответствие видов документации их назначению</td><td>А - 2, Б - 1, В - 3.</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td></td><td></td><td>испытаний системы защиты информации</td><td><table><tr><td>Документ</td><td>Что определяет или фиксирует</td></tr><tr><td>А) Программа испытаний</td><td>1) Описание конкретных шагов и действий для проверки СЗИ</td></tr><tr><td>Б) Методика испытаний</td><td>2) Перечень объектов, объем, сроки и условия проведения проверок</td></tr><tr><td>В) Протокол испытаний</td><td>3) Результаты выполнения каждой проверки и выявленные отклонения</td></tr></table></td><td></td></tr>
<tr><td colspan="5">Задание закрытого типа на установление последовательности (проверяет эксперт)</td></tr>
<tr><td>3</td><td>309.</td><td>Ввод системы защиты информации в эксплуатацию</td><td>Установите правильную последовательность этапов испытаний СЗИ перед их окончательной приемкой в эксплуатацию:
1. Опытная эксплуатация системы.
2. Предварительные испытания (проверка работоспособности).
3. Приемочные испытания (итоговая проверка).
4. Заводские испытания (проверка отдельных компонентов разработчиком).</td><td>4, 2, 1, 3.</td></tr>
<tr><td>3</td><td>310.</td><td>Ввод системы защиты информации в эксплуатацию</td><td>Расположите этапы ввода СЗИ в эксплуатацию в государственных информационных системах (ГИС) в соответствии с требованиями регуляторов:
1. Проведение аттестационных испытаний объекта.
2. Установка и настройка средств защиты информации.
3. Выдача аттестата соответствия по требованиям безопасности.
4. Издание приказа о вводе системы в промышленную эксплуатацию.</td><td>2, 1, 3, 4.</td></tr>
<tr><td>3</td><td>311.</td><td>Организация приемочных испытаний системы защиты информации</td><td>Установите правильную последовательность этапов организации приемочных испытаний системы защиты информации:
1. Формирование приемочной комиссии и издание соответствующего приказа.
2. Подготовка испытательного стенда и проверка комплектности СЗИ.
3. Разработка и согласование Программы и методики испытаний (ПМИ).
4. Анализ исходных требований технического задания (ТЗ) и проектных решений.</td><td>4, 3, 1, 2.</td></tr>
<tr><td>3</td><td>312.</td><td>Организация приемочных испытаний системы защиты информации</td><td>Установите последовательность действий при завершении приемочных испытаний и оформлении результатов:
1. Оформление итогового Акта о приемке СЗИ в эксплуатацию.
2. Составление протоколов по каждому разделу программы испытаний.
3. Устранение разработчиком выявленных замечаний и недостатков (при наличии).</td><td>2, 4, 3, 1.</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			4. Формирование перечня замечаний и предложений по доработке системы.	
Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)				
4	313.	Производственная, Организационно-управленческая практика	Вам поручено организовать и провести приемочные испытания системы защиты от несанкционированного доступа (СЗИ от НСД), установленной на автоматизированное рабочее место. Сформулируйте один простой сценарий проверки для приемочных испытаний.	*Цель:* Убедиться, что СЗИ блокирует загрузку операционной системы при изменении контролируемого файла. *Действие:* Администратор безопасности намеренно вносит изменения в один из системных файлов, поставленных на контроль целостности в СЗИ, и перезагружает компьютер. *Ожидаемый результат:* СЗИ от НСД при загрузке выявляет модификацию файла, блокирует дальнейший старт операционной системы и выводит сообщение о нарушении целостности среды. Данный факт заносится в протокол испытаний.
4	314.	Производственная, Организационно-управленческая практика	Вам поручено организовать и провести приемочные испытания системы защиты от несанкционированного доступа (СЗИ от НСД), установленной на автоматизированное рабочее место. Опишите итоговое действие для официального ввода данной СЗИ в эксплуатацию.	1. После успешного завершения всех проверок по программе и методике испытаний оформляется «Акт завершения приемочных испытаний». 2. На основании акта разрабатывается и подписывается руководством предприятия «Приказ о вводе СЗИ от НСД в промышленную эксплуатацию».
4	315.	Производственная, Преддипломная практика	Опишите процедуру тестирования системы обнаружения вторжений (СОВ).	Имитация типовых атак и фиксация срабатывания оповещений в журнале событий.
4	316.	Производственная, Преддипломная практика	Составьте акт ввода в эксплуатацию подсистемы антивирусной защиты.	Подтверждение корректности установки на все узлы и настройки централизованного обновления баз.
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
3	317.	Ввод системы защиты информации в эксплуатацию	Этап ввода СЗИ в эксплуатацию, в ходе которого осуществляется проверка работоспособности системы в реальных условиях и обучение персонала работе с ней, называется _____ эксплуатация.	Опытная
3	318.	Ввод системы защиты	Итоговый документ, подтверждающий, что объект информатизации	Аттестат

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
		информации в эксплуатацию	соответствует требованиям стандартов и нормативных документов по безопасности информации, называется _____ соответствия.	
3	319.	Ввод системы защиты информации в эксплуатацию	Процесс официального подтверждения готовности системы к использованию по назначению, завершающийся изданием руководителем организации _____ о вводе в эксплуатацию.	Приказа
3	320.	Ввод системы защиты информации в эксплуатацию	При проведении приемочных испытаний проверяется наличие у используемых средств защиты информации действующих _____ соответствия (ФСТЭК или ФСБ России).	Сертификатов
3	321.	Организация приемочных испытаний системы защиты информации	Коллегиальный орган, назначаемый приказом руководителя для проведения проверки соответствия системы защиты информации (СЗИ) требованиям технического задания и принятия решения о её приемке, называется приемочная _____.	комиссия
3	322.	Организация приемочных испытаний системы защиты информации	Документально зафиксированные сведения о выявленных в ходе испытаний отказах, сбоях или несоответствиях СЗИ проектным решениям называются перечнем _____.	замечаний (или недостатков).
3	323.	Организация приемочных испытаний системы защиты информации	Проверка СЗИ, проводимая с целью подтверждения того, что программное обеспечение не было изменено в процессе поставки и установки, называется контролем _____.	целостности
3	324.	Организация приемочных испытаний системы защиты информации	Этап испытаний, проводимый непосредственно перед приемочными испытаниями для определения готовности системы к опытной эксплуатации, называется _____ испытаниями.	предварительными
Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора				
4	325.	Производственная, Организационно-управленческая практика	При приемочных испытаниях системы контроля доступа (СКУД) выяснилось, что при отключении электропитания все замки на дверях остаются заблокированными, препятствуя эвакуации. Какое решение принять? 1. Принять систему, так как это обеспечивает максимальный уровень защиты от злоумышленников. 2. Отклонить приемку СЗИ и выставить требование подрядчику настроить автоматическую разблокировку замков при пропадании питания или срабатывании пожарной тревоги. 3. Принять систему и выдать всем сотрудникам по топору на случай пожара. 4. Изменить ТЗ, указав, что эвакуация из здания не предусмотрена.	2 Приемочные испытания систем физической и информационной безопасности не должны противоречить нормам охраны труда и пожарной безопасности.
4	326.	Производственная, Организационно-управленческая практика	Вы успешно завершили все тесты межсетевого экрана по Программе и методике испытаний (ПМИ). Что является финальным шагом для его ввода в промышленную эксплуатацию?	3 Официальный ввод СЗИ в эксплуатацию на предприятии — это

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			1. Устное поздравление команды инженеров. 2. Отправка электронного письма всем сотрудникам о том, что теперь всё защищено. 3. Подписание Акта завершения приемочных испытаний членами комиссии и издание руководителем Приказа о вводе СЗИ в эксплуатацию. 4. Перезагрузка межсетевого экрана.	юридически значимое действие, требующее документальной фиксации ответственности в виде актов и приказов.
4	327.	Производственная, Преддипломная практика	«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования вы выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Перед аттестацией обязательно проводятся приемочные испытания и ввод СЗИ в эксплуатацию, чтобы убедиться, что средства защиты настроены корректно и выполняют свои функции.
4	328.	Производственная, Преддипломная практика	При приемочных испытаниях системы защиты от НСД обнаружено, что она блокирует доступ пользователям, имеющим законные права. О чем это говорит? 1. О слишком высокой надежности системы. 2. О некорректной настройке правил разграничения доступа, требующей доработки системы перед вводом. 3. О том, что пользователи пытаются взломать систему. 4. О неисправности клавиатуры.	2. Приемочные испытания проверяют соответствие системы техническому заданию (ТЗ). Ошибочная блокировка легитимных пользователей мешает бизнес-процессам и свидетельствует о неготовности СЗИ к эксплуатации.

ПК-6 Прогнозирует риски в информационной безопасности и управляет инцидентами информационной безопасности

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
Задание закрытого типа с выбором одного/нескольких правильного ответа из предложенных				
1	329.	Построение моделей угроз информационной безопасности	Что НЕ относится к категориям угроз: 1. по масштабу; 2. по характеру ущерба; 3. расположение источника; 4. по скорости возникновения.	4
1	330.	Построение моделей угроз информационной безопасности	Укажите адрес информационного сайта на котором размещены общий перечень угроз безопасности информации, содержащейся в банке данных угроз безопасности информации ФСТЭК России: 1. fsb.ru 2. bdu.fstec.ru 3. бду.фстэк.рф 4. cert.gov.ru/o-nktski	2
1	331.	Построение моделей угроз информационной безопасности	Какой этап не входит в оценку угроз безопасности информации? 1. определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации; 2. определение возможных объектов воздействия угроз безопасности информации; 3. оценку возможности реализации (возникновения) угроз безопасности информации и определение их актуальности; 4. определение лиц информационного взаимодействия.	4
1	332.	Построение моделей угроз информационной безопасности	По результатам определения источников угроз безопасности информации должны быть определены (множественный выбор): 1. виды актуальных нарушителей и возможные цели реализации ими угроз безопасности информации, а также их возможности; 2. список программного обеспечения; 3. категории актуальных нарушителей, которые могут реализовать угрозы безопасности информации; 4. страну происхождения программных продуктов и программных комплексов.	1, 3
Задание закрытого типа на установление соответствия (проверяет эксперт)				

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td>1</td><td>333.</td><td>Построение моделей угроз информационной безопасности</td><td>Сопоставьте название нормативно-правовых актов с их реквизитами<table><tr><td>А. №149-ФЗ от 27.07.2006 г.</td><td>1. Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений</td></tr><tr><td>Б. №187-ФЗ от 26.07.2017 г.</td><td>2. О персональных данных</td></tr><tr><td>В. №152-ФЗ от 27.07.2006 г.</td><td>3. О безопасности критической информационной инфраструктуры Российской Федерации</td></tr><tr><td>Г. №117 от 11.04.2025 г.</td><td>4. Об информации, информационных технологиях и о защите информации</td></tr></table></td><td>А-4, Б-3, В-2, Г-1</td></tr>
<tr><td>1</td><td>334.</td><td>Построение моделей угроз информационной безопасности</td><td>Установите соответствие стратегий управления рисками и защитных мер<table><tr><td>Стратегия</td><td>Пример реализации в модели</td></tr><tr><td>А) Снижение риска</td><td>1) Отказ от использования беспроводных сетей в организации</td></tr><tr><td>Б) Избегание риска</td><td>2) Установка системы обнаружения вторжений (IDS)</td></tr><tr><td>В) Передача риска</td><td>3) Страхование ответственности за утечку данных</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
<tr><td>1</td><td>335.</td><td>Построение моделей угроз информационной безопасности</td><td>Установите соответствие методов оценки и их специфики<table><tr><td>Метод оценки риска</td><td>Специфика подхода</td></tr><tr><td>А) Качественный</td><td>1) Расчет ущерба в денежном эквиваленте (рубли, доллары)</td></tr><tr><td>Б) Количественный</td><td>2) Оценка по шкале «высокий / средний / низкий»</td></tr><tr><td>В) Комбинированный</td><td>3) Использование балльных оценок вместе с финансовым прогнозом</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
</table>

<table>
<tr><th>Семестр</th><th>Номер задания</th><th>Наименование дисциплины</th><th>Содержание вопроса (задания)</th><th>Правильный ответ</th></tr>
<tr><td>1</td><td>336.</td><td>Построение моделей угроз информационной безопасности</td><td>Установите соответствие видов последствий и нарушаемых свойств информации<table><tr><td>Тип последствия</td><td>Нарушаемое свойство</td></tr><tr><td>А) Опубликование персональных данных в сети</td><td>1) Целостность</td></tr><tr><td>Б) Удаление базы данных без возможности восстановления</td><td>2) Конфиденциальность</td></tr><tr><td>В) Подмена суммы транзакции в банковской системе</td><td>3) Доступность</td></tr></table></td><td>А - 2, Б - 3, В - 1.</td></tr>
<tr><td>1</td><td>337.</td><td>Построение моделей угроз информационной безопасности</td><td>Установите соответствие уровней актуальности угроз (по методике ФСТЭК) и их описания<table><tr><td>Уровень актуальности</td><td>Описание</td></tr><tr><td>А) Актуальная угроза</td><td>1) Малая вероятность реализации и низкая степень ущерба</td></tr><tr><td>Б) Неактуальная угроза</td><td>2) Высокая вероятность реализации или значительный ущерб</td></tr><tr><td>В) Потенциальная угроза</td><td>3) Теоретически возможная угроза без привязки к конкретной системе</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
<tr><td>1</td><td>338.</td><td>Построение моделей угроз информационной безопасности</td><td>Установите соответствие компонентов риска и их определений<table><tr><td>Компонент</td><td>Определение</td></tr><tr><td>А) Угроза</td><td>1) Слабое место в защите или ошибка в программном коде</td></tr><tr><td>Б) Уязвимость</td><td>2) Потенциальная возможность нарушения безопасности информации</td></tr><tr><td>В) Ущерб</td><td>3) Негативные последствия реализации угроз (финансовые, репутационные)</td></tr></table></td><td>А - 2, Б - 1, В - 3.</td></tr>
<tr><td colspan="5">Задание закрытого типа на установление последовательности (проверяет эксперт)</td></tr>
<tr><td>1</td><td>339.</td><td>Построение моделей угроз информационной безопасности</td><td>Установите последовательность действий при анализе модели нарушителя:
1. Определение категории нарушителя (внутренний/внешний).
2. Оценка потенциала и ресурсов нарушителя (низкий, средний, высокий).
3. Описание вероятных целей нарушителя.</td><td>1, 3, 2, 4.</td></tr>
</table>

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
			4. Определение доступных нарушителю точек входа в систему.	
1	340.	Построение моделей угроз информационной безопасности	Расставьте шаги оценки рисков ИБ в логической последовательности: 1. Идентификация ценных активов и их уязвимостей. 2. Расчет вероятности реализации угроз. 3. Определение величины потенциального ущерба. 4. Сравнение расчетного уровня риска с допустимым порогом.	1, 3, 2, 4.
1	341.	Построение моделей угроз информационной безопасности	Установите порядок действий нарушителя при реализации атаки в модели: 1. Эксплуатация выявленной уязвимости. 2. Разведка и поиск слабых мест в защите. 3. Достижение конечной цели (хищение или порча данных). 4. Закрепление в системе и повышение привилегий.	2, 1, 4, 3.
1	342.	Построение моделей угроз информационной безопасности	Установите последовательность действий при управлении рисками после их оценки: 1. Выбор стратегии обработки (снижение, перенос, принятие, избегание). 2. Разработка плана внедрения дополнительных мер защиты. 3. Оценка остаточного уровня риска. 4. Утверждение итоговой модели руководством.	1, 2, 3, 4.
1	343.	Построение моделей угроз информационной безопасности	Расположите действия эксперта для определения актуальности угрозы: 1. Определение частоты возникновения угрозы в аналогичных системах. 2. Оценка технической возможности реализации угрозы в текущей архитектуре. 3. Определение уровня ущерба для бизнес-процессов. 4. Принятие решения об актуальности (актуальна / не актуальна).	2, 1, 3, 4.
1	344.	Построение моделей угроз информационной безопасности	Установите последовательность действий при переходе от прогнозирования к реагированию: 1. Разработка сценариев реагирования на прогнозируемые угрозы. 2. Включение сценариев в инструкции персонала по управлению инцидентами. 3. Определение признаков (индикаторов) срабатывания угрозы в модели. 4. Мониторинг событий безопасности на основе модели.	3, 1, 2, 4.
Задание открытого типа с развернутым ответом/ задача (проверяет эксперт)				
3	345.	Производственная, Организационно-управленческая практика	В журнале событий межсетевого экрана зафиксирована аномалия: в нерабочее время (в 02:00 ночи) произошла выгрузка 50 Гб данных с корпоративного файлового сервера на неизвестный внешний IP-адрес. Спрогнозируйте риски.	Критический риск утечки конфиденциальной информации, нарушение требований законодательства и регуляторов, финансовые и репутационные потери.
3	346.	Производственная,	В журнале событий межсетевого экрана зафиксирована аномалия: в	▪ Локализация.

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
		Организационно-управленческая практика	нерабочее время (в 02:00 ночи) произошла выгрузка 50 Гб данных с корпоративного файлового сервера на неизвестный внешний IP-адрес. Опишите порядок управления этим инцидентом	▪ Анализ. ▪ Устранение и восстановление. ▪ Документирование.
4	347.	Производственная, Преддипломная практика	Спрогнозируйте риски при использовании администраторами общих учетных записей.	Невозможность персонализации ответственности при инциденте; риск несанкционированного изменения настроек без следа.
4	348.	Производственная, Преддипломная практика	Разработайте алгоритм действий при обнаружении массовой рассылки фишинговых писем.	Блокировка адреса отправителя, удаление писем из почтовых ящиков, принудительный сброс паролей скомпрометированных пользователей.
Задания открытого типа с кратким ответом/ вставить термин, словосочетание….., дополнить предложенное (проверяет эксперт)				
1	349.	Построение моделей угроз информационной безопасности	_____ - это нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации	внешние нарушители
1	350.	Построение моделей угроз информационной безопасности	___– это потенциальная возможность определенным образом нарушить информационную безопасность	угроза
1	351.	Построение моделей угроз информационной безопасности	___– это попытка реализации угрозы	атака
1	352.	Построение моделей угроз информационной безопасности	___– это состояние, в котором находится объект безопасности вследствие возникновения угрозы этому объекту	опасность
1	353.	Построение моделей угроз информационной безопасности	___ - это промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется	окно опасности
1	354.	Построение моделей угроз информационной безопасности	Показатель, определяемый как произведение вероятности реализации угрозы и величины возможного ущерба для организации, называется _____ информационной безопасности.	риском
1	355.	Построение моделей угроз информационной безопасности	Недостаток или слабое место в системе защиты, программном обеспечении или аппаратных средствах, которое может быть использовано нарушителем для реализации угрозы, называется _____.	уязвимостью
1	356.	Построение моделей угроз	Совокупность условий и факторов, создающих потенциальную или реально	угрозой

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
		информационной безопасности	существующую опасность нарушения безопасности информации, называется _____ информационной безопасности.	
Задания комбинированного типа с выбором одного/нескольких правильного ответа из предложенных с последующим объяснением своего выбора				
3	357.	Производственная, Организационно-управленческая практика	Антивирусная система на сервере внезапно начала фиксировать массовое и быстрое изменение расширений сотен файлов на ".locked". Спрогнозируйте риск и выберите действие. 1. Это плановое архивирование данных системой; ничего делать не нужно. 2. Риск поломки жесткого диска; нужно немедленно перезагрузить сервер. 3. Риск атаки вируса-шифровальщика; необходимо немедленно изолировать сервер от сети и остановить подозрительные процессы. 4. Риск сбоя в базе данных; нужно запустить проверку диска.	3 Прогнозирование рисков позволяет вовремя распознать паттерн поведения шифровальщика. Первым шагом локализации инцидента является отключение от сети для спасения остальных узлов инфраструктуры.
3	358.	Производственная, Организационно-управленческая практика	При прогнозировании рисков вы понимаете, что единственный системный администратор компании знает все пароли наизусть и нигде их не фиксирует. Какое управленческое решение снизит этот риск? 1. Заставить администратора сдать экзамен на память. 2. Уволить администратора, пока он ничего не забыл. 3. Внедрить систему управления паролями (менеджер паролей) с разделением прав и регламентировать обязательное документирование учетных записей. 4. Ничего не делать, так как администратор работает в компании уже 10 лет.	3 Снижение риска потери критических знаний и монополизации доступа достигается за счет внедрения специализированных инструментов хранения паролей и регламентации процессов документирования.
4	359.	Производственная, Преддипломная практика	«Подготовка объекта к обработке сведений, составляющих государственную тайну». В ходе преддипломной практики вам поручено подготовить к эксплуатации выделенное помещение (ВП) и автоматизированную систему (АС) для работы со сведениями под грифом «Секретно». На этапе обследования вы выяснили, что стена помещения является смежной с коридором общего пользования, а на компьютерах не установлены средства защиты от несанкционированного доступа (СЗИ от НСД). Какая последовательность действий является методологически верной для успешного прохождения аттестации и ввода объекта в эксплуатацию? Варианты ответа: 1. Сначала установить антивирус, затем пригласить аттестационную комиссию, а проблему со смежной стеной решить после получения аттестата. 2. Провести предпроектное обследование, обосновать установку системы виброакустической защиты и СЗИ от НСД, разработать документы согласно нормам СТР, провести приемочные испытания установленных средств и передать объект на аттестацию. 3. Написать научную статью о методах взлома защищенных стен, закупить любое зарубежное ПО для шифрования дисков и составить график дежурств сотрудников в коридоре для охраны стены	2 Устранение уязвимости стены на этапе проектирования - это предотвращение перехвата информации по виброакустическому каналу.

Семестр	Номер задания	Наименование дисциплины	Содержание вопроса (задания)	Правильный ответ
4	360.	Производственная, Преддипломная практика	Система мониторинга зафиксировала 500 попыток входа под именем "admin" с внешнего IP-адреса за одну минуту. К какому типу инцидентов это относится? 1. Плановое обновление системы. 2. Инцидент типа «Brute-force» (подбор пароля), требующий немедленной блокировки IP-адреса. 3. Пользователь просто забыл пароль и часто нажимает Enter. 4. Технический сбой в работе сетевой карты.	2. Умение прогнозировать риски позволяет отличить штатную активность от аномальной. Массовые попытки авторизации - классический инцидент ИБ, требующий стандартного алгоритма реагирования для предотвращения взлома.