МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И.о. декана факультета математики и компьютерных наук имени профессора Н.И. Червякова
Т.А. Гробова
Ф.И.О.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Основы управления информационной безопасностью
название дисциплины (модуля)

Направление подготовки	10.03.01 «Информационная безопасность»
Направленность (профиль)	Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестре	8

Введение

1. Назначение. Фонд оценочных средств (ФОС) предназначен для текущего контроля успеваемости и промежуточной аттестации по дисциплине «Основы управления информационной безопасностью» студентов, обучающихся по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

2. ФОС является приложением к программе дисциплины (модуля) «Основы управления информационной безопасностью» в соответствии с образовательной программой высшего образования по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)».

3. Разработчик (и) Жук А.П., профессор кафедры

4. Проведена экспертиза ФОС.
Члены экспертной группы:
Председатель: Петренко В.И., заведующий кафедрой
Члены комиссии: Жук А.П., профессор кафедры
Минкина Т.В., доцент кафедры

Представитель организации-работодателя Демурчев Н.Г., директор ООО «СГУ-Инфоком»

Экспертное заключение: Фонд оценочных средств соответствует ОП ВО по направлению подготовки 10.03.01 «Информационная безопасность», направленность (профиль) «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Основы управления информационной безопасностью».

5. Срок действия ФОС определяется сроком реализации образовательной программы.

1. Описание критериев оценивания компетенции на различных этапах их формирования, описание шкал оценивания

Компетенция (ии), индикатор (ы)	Уровни сформированности компетенции(й),			
	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Минимальный уровень не достигнут (неудовлетворительно) 2 балла	Высокий уровень (отлично) 5 баллов
Компетенция: **ОПК-5** - Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;				
Результаты обучения по дисциплине (модулю): Индикатор: **ИД-2** ОПК-5 Определяет рациональные меры по обеспечению организационной защите на объекте; организует работу персонала с конфиденциальной информацией; разрабатывает проекты нормативных документов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядитель	не составляет и не использует нормативные и методические документы, регламентирующие деятельность по защите информации на предприятии в минимально-допустимом объеме	составляет и использует нормативные и методические документы, регламентирующие деятельность по защите информации на предприятии в минимально-допустимом объеме	составляет и использует основные нормативные и методические документы, регламентирующие деятельность по защите информации на предприятии	составляет и использует известные нормативные и методические документы, регламентирующие деятельность по защите информации на предприятии

ных документов				
Компетенция: ***ОПК-10*** Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;				
Результаты обучения по дисциплине (модулю): Индикатор: **ИД-1** ОПК-10 Использует методологический базис теории защиты информации, используемый при разработке формировании политики информационной безопасности	не уверенно использует методологический базис теории защиты информации, используемый при разработке формировании политики информационной безопасности	не в полной мере использует методологический базис теории защиты информации, используемый при разработке формировании политики информационной безопасности	в целом использует методологический базис теории защиты информации, используемый при разработке формировании политики информационной безопасности	уверенно использует методологический базис теории защиты информации, используемый при разработке формировании политики информационной безопасности
Результаты обучения по дисциплине (модулю): Индикатор: **ИД-2** ОПК-10 Осуществляет организацию и поддерживает выполнение комплекса мер по обеспечению информационной безопасности на объекте защиты в качестве технического специалиста	не уверенно осуществляет организацию и поддерживает выполнение комплекса мер по обеспечению информационной безопасности на объекте защиты в качестве технического специалиста	не в полной мере осуществляет организацию и поддерживает выполнение комплекса мер по обеспечению информационной безопасности на объекте защиты в качестве технического специалиста	в целом осуществляет организацию и поддерживает выполнение комплекса мер по обеспечению информационной безопасности на объекте защиты в качестве технического специалиста	уверенно осуществляет организацию и поддерживает выполнение комплекса мер по обеспечению информационной безопасности на объекте защиты в качестве технического специалиста
Результаты обучения по дисциплине (модулю): Индикатор: **ИД-3** ОПК-10	не уверенно управляет процессом выполнения комплекса мер	не в полной мере управляет процессом выполнения комплекса мер	в целом управляет процессом выполнения комплекса мер	уверенно управляет процессом выполнения комплекса мер по

Управляет процессом выполнения комплекса мер по обеспечению информационной безопасности реализации на объекте защиты в качестве технического специалиста	по обеспечению информационной безопасности реализации на объекте защиты в качестве технического специалиста	по обеспечению информационной безопасности реализации на объекте защиты в качестве технического специалиста	по обеспечению информационной безопасности реализации на объекте защиты в качестве технического специалиста	обеспечению информационной безопасности реализации на объекте защиты в качестве технического специалиста
Компетенция: **ОПК-2.4** Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;				
Результаты обучения по дисциплине (модулю): Индикатор: **ИД-1** Организует мероприятия по аудиту защищенности объекта информатизации в соответствии с нормативными документами (Основы управления информационной безопасностью)	не организует минимально-допустимый объем мероприятий по аудиту защищенности объекта информатизации в соответствии с нормативными документами	организует минимально-допустимый объем мероприятий по аудиту защищенности объекта информатизации в соответствии с нормативными документами	организует основные мероприятия по аудиту защищенности объекта информатизации в соответствии с нормативными документами	организует все мероприятия по аудиту защищенности объекта информатизации в соответствии с нормативными документами
Результаты обучения по дисциплине (модулю): Индикатор: **ИД-2** Проводит аудит защищенности объекта	не проводит минимально-допустимый объем мероприятий по аудиту защищенности объекта информатизации	проводит минимально-допустимый объем мероприятий по аудиту защищенности объекта информатизации в	проводит основные мероприятия по аудиту защищенности объекта информатизации в соответствии с нормативными документами	проводит все мероприятия по аудиту защищенности объекта информатизации в соответствии с нормативным

информатизации в соответствии с нормативными документами (Основы управления информационной безопасностью)	в соответствии с нормативными документами	соответствии с нормативными документами		и документами

Оценивание уровня сформированности компетенции по дисциплине осуществляется на основе «Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры - в федеральном государственном автономном образовательном учреждении высшего образования «Северо-Кавказский федеральный университет» в актуальной редакции.

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕРКИ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Номер задания	Правильный ответ	Содержание вопроса	Компетенция
		Форма обучения ОФО семестр 8	
1.		Дайте понятие информационной безопасности в узком и широком смысле слова.	ОПК-5 ОПК-10 ОПК-2.4
2.		Дайте определение рисков и охарактеризуйте их виды.	ОПК-5 ОПК-10 ОПК-2.4
3.		Дайте определение угроз и охарактеризуйте их виды.	ОПК-5 ОПК-10 ОПК-2.4
4.		Охарактеризуйте основные наиболее распространенные способы нарушения информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
5.		Охарактеризуйте процесс обеспечения собственной информационной безопасности на предприятиях.	ОПК-5 ОПК-10 ОПК-2.4
6.		Укажите основные международные организации, действующие в сфере информационной безопасности и укажите решаемые ими задачи.	ОПК-5 ОПК-10 ОПК-2.4
7.		Опишите отличительные особенности крупных международных профессиональных (отраслевых) организаций (объединений).	ОПК-5 ОПК-10 ОПК-2.4
8.		Назначение, структура и сфера деятельности International Telecommunication Union (ITU) – Международного союза электросвязи.	ОПК-5 ОПК-10 ОПК-2.4
9.		Назначение, структура и сфера деятельности International Telecommunication Union (ITU) – Международного союза электросвязи.	ОПК-5 ОПК-10 ОПК-2.4
10.		Дайте определение системы управления информационной безопасностью (СУИБ) предприятия, приведите её состав и цели создания.	ОПК-5 ОПК-10 ОПК-2.4

11.		Основные этапы и условия разработки СУИБ.	ОПК-5 ОПК-10 ОПК-2.4
12.		Охарактеризуйте этап разработки СУИБ: Инвентаризация активов компании.	ОПК-5 ОПК-10 ОПК-2.4
13.		Охарактеризуйте этап разработки СУИБ: Категорирование активов компании.	ОПК-5 ОПК-10 ОПК-2.4
14.		Охарактеризуйте этап разработки СУИБ: Оценка защищенности информационной системы.	ОПК-5 ОПК-10 ОПК-2.4
15.		Охарактеризуйте этапы определения политики безопасности предприятия.	ОПК-5 ОПК-10 ОПК-2.4
16.		Опишите организационную структуру менеджмента обеспечения информационной безопасности предприятия.	ОПК-5 ОПК-10 ОПК-2.4
17.		Основные функции отдела информационной безопасности предприятия.	ОПК-5 ОПК-10 ОПК-2.4
18.		Сценарий анализа информационных рисков компании.	ОПК-5 ОПК-10 ОПК-2.4
19.		Дайте определение и поясните смысл политики безопасности предприятия.	ОПК-5 ОПК-10 ОПК-2.4
20.		Приведите схему управления безопасностью информационных технологий.	ОПК-5 ОПК-10 ОПК-2.4
21.		Поясните основные этапы управления безопасностью информационных технологий.	ОПК-5 ОПК-10 ОПК-2.4
22.		Опишите процедуру оценки общего уровня риска при управлении безопасностью информационных технологий.	ОПК-5 ОПК-10 ОПК-2.4
23.		Порядок оценки важности информационные технологий для функционирования организации.	ОПК-5 ОПК-10 ОПК-2.4

24.		Дайте определение и раскройте задачи, решаемые департаментом информационной безопасности предприятия (ДИБП).	ОПК-5 ОПК-10 ОПК-2.4
25.		Опишите функции ДИБП, связанные с формированием, поддержкой и документальным обеспечением политики информационной безопасности предприятия.	ОПК-5 ОПК-10 ОПК-2.4
26.		Опишите функции ДИБП, с внедрением средств защиты информации.	ОПК-5 ОПК-10 ОПК-2.4
27.		Опишите функции ДИБП, связанные с администрированием информационных систем и систем защиты информации.	ОПК-5 ОПК-10 ОПК-2.4
28.		Дайте определение аудита состояния информационной безопасности предприятия. Охарактеризуйте их виды.	ОПК-5 ОПК-10 ОПК-2.4
29.		Опишите цели и стратегическую задачу аудита состояния информационной безопасности предприятия.	ОПК-5 ОПК-10 ОПК-2.4
30.		Опишите требования к организациям, осуществляющим внешний аудит состояния информационной безопасности предприятия.	ОПК-5 ОПК-10 ОПК-2.4
31.		Основные этапы аудита состояния информационной безопасности предприятия и их характеристика.	ОПК-5 ОПК-10 ОПК-2.4
32.		Охарактеризуйте процесс анализа действующей на предприятии политики безопасности.	ОПК-5 ОПК-10 ОПК-2.4
33.		Охарактеризуйте процесс изучения (проверки) действующих информационных ресурсов предприятия.	ОПК-5 ОПК-10 ОПК-2.4

34.		Каким образом обеспечивается программная поддержка реализации политики информационной безопасности и основные функции специальных программных продуктов.	ОПК-5 ОПК-10 ОПК-2.4
35.		Виды программных средств поддержки реализации политики информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
36.		Дайте характеристику сборников - программных средств поддержки реализации политики информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
37.		Дайте характеристику программного продукта «COBRA» и его базового модуля.	ОПК-5 ОПК-10 ОПК-2.4
38.		Структура и краткое содержание отчета о состоянии информационной безопасности программного продукта «COBRA».	ОПК-5 ОПК-10 ОПК-2.4
39.		Дайте характеристику программного комплекса управления политикой информационной безопасности компании «КОНДОР+».	ОПК-5 ОПК-10 ОПК-2.4
40.		Дайте понятие инцидента в сфере информационной безопасности и причины его обуславливающие.	ОПК-5 ОПК-10 ОПК-2.4
41.		Охарактеризуйте организационные процедуры (регламенты) реагирования на инциденты.	ОПК-5 ОПК-10 ОПК-2.4
42.		Дайте характеристику этапа обнаружение нападения при реагировании на инциденты.	ОПК-5 ОПК-10 ОПК-2.4
43.		Дайте характеристику этапа локализация нападения при реагировании на инциденты.	ОПК-5 ОПК-10 ОПК-2.4

44.		Охарактеризуйте предпосылки для формирования рынка различных услуг по обеспечению информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
45.		Достоинства и недостатки применения аутсорсинга в сфере информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
46.		Основные виды услуг, которые могут быть переданы на аутсорсинг в сфере информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
47.		Дайте характеристику услуги по реагированию на инциденты (нарушения информационной безопасности).	ОПК-5 ОПК-10 ОПК-2.4
48.		Дайте характеристику услуги аудита информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
49.		Дайте характеристику услуги проверки защищенности и надежности отдельных элементов информационной инфраструктуры.	ОПК-5 ОПК-10 ОПК-2.4
50.		Основные задачи организационной работы крупных (т.е. занимающих большую долю рынка) поставщиков широко используемых информационных систем в сфере информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
51.		Организационная работа в сфере информационной безопасности на уровне крупных компаний.	ОПК-5 ОПК-10 ОПК-2.4
52.		Внутренняя организационная работа по обеспечению информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
53.		Основные приемы и методы внешней организационной работы в сфере информационной безопасности на уровне крупных компаний–поставщиков информационных систем.	ОПК-5 ОПК-10 ОПК-2.4

54.		Внутренняя организационная работа в сфере информационной безопасности продуктов корпорации Microsoft.	ОПК-5 ОПК-10 ОПК-2.4
55.		Предпосылки развития государственного управления в сфере информационной безопасности	ОПК-5 ОПК-10 ОПК-2.4
56.		Характеристика факторов, определяющих состояние информационной безопасности государства.	ОПК-5 ОПК-10 ОПК-2.4
57.		Общая методология и структура организационного обеспечения информационной безопасности на уровне государств.	ОПК-5 ОПК-10 ОПК-2.4
58.		Предпосылки разработки политики безопасности предприятия.	ОПК-5 ОПК-10 ОПК-2.4
59.		Структура деятельности в сфере информационной безопасности. Основные задачи организационно-управленческой деятельности (менеджмента) в сфере информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
60.		Что включает в себя безопасная информационная инфраструктура?	ОПК-5 ОПК-10 ОПК-2.4
61.		Иерархия уровней организационной работы в сфере информационной безопасности и их характеристика.	ОПК-5 ОПК-10 ОПК-2.4
62.		Назначение, структура и сфера деятельности World Wide Web Consortium (W3C) – Консорциума Всемирной Паутины.	ОПК-5 ОПК-10 ОПК-2.4
63.		Назначение, структура и сфера деятельности International Organization for Standardization (ISO) – Международной организации по стандартизации.	ОПК-5 ОПК-10 ОПК-2.4
64.		Назначение, структура и сфера деятельности CERT Coordination Center (CERT/CC) – Координационный центр CERT в области управления информационной	ОПК-5 ОПК-10 ОПК-2.4

		безопасностью.	
65.		Назначение, структура и сфера деятельности X-Force security intelligence team – Исследовательской группы X-Force.	ОПК-5 ОПК-10 ОПК-2.4
66.		Охарактеризуйте этап разработки СУИБ: Оценка информационных рисков.	ОПК-5 ОПК-10 ОПК-2.4
67.		Охарактеризуйте этап разработки СУИБ: Обработка информационных рисков .	ОПК-5 ОПК-10 ОПК-2.4
68.		Охарактеризуйте этап разработки СУИБ: Внедрение выбранных мер обработки рисков.	ОПК-5 ОПК-10 ОПК-2.4
69.		Охарактеризуйте этап разработки СУИБ: Контроль выполнения и эффективности выбранных мер.	ОПК-5 ОПК-10 ОПК-2.4
70.		Охарактеризуйте верхний уровень политики информационной безопасности предприятия.	ОПК-5 ОПК-10 ОПК-2.4
71.		Охарактеризуйте средний уровень политики информационной безопасности предприятия.	ОПК-5 ОПК-10 ОПК-2.4
72.		Охарактеризуйте нижний уровень политики информационной безопасности предприятия.	ОПК-5 ОПК-10 ОПК-2.4
73.		Общий жизненный цикл политики информационной безопасности предприятия.	ОПК-5 ОПК-10 ОПК-2.4
74.		Основные положения стратегии безопасности информационных технологий.	ОПК-5 ОПК-10 ОПК-2.4
75.		Перечислите должностных лиц предприятия, которые должны принимать участие при разработке политики безопасности информационных технологий.	ОПК-5 ОПК-10 ОПК-2.4

76.		Что должно включать в себя описание политики обеспечения безопасности информационных технологий?	ОПК-5 ОПК-10 ОПК-2.4
77.		Приведите перечень основных вопросов, входящих в состав политики безопасности информационных технологий.	ОПК-5 ОПК-10 ОПК-2.4
78.		Опишите функции ДИБП, связанные с контролем выполнения требований политики информационной безопасности и проведением аудитов.	ОПК-5 ОПК-10 ОПК-2.4
79.		Опишите функции ДИБП, связанные с охраной имущества предприятия.	ОПК-5 ОПК-10 ОПК-2.4
80.		Приведите вариант организационной схемы ДИБП.	ОПК-5 ОПК-10 ОПК-2.4
81.		Содержание работы аудиторов в процессе сбора информации.	ОПК-5 ОПК-10 ОПК-2.4
82.		Проверка состояния физической безопасности информационной инфраструктуры.	ОПК-5 ОПК-10 ОПК-2.4
83.		Инструментальная проверка защищенности информационной системы предприятия.	ОПК-5 ОПК-10 ОПК-2.4
84.		Анализ собранной информации при аудите состояния информационной безопасности предприятия.	ОПК-5 ОПК-10 ОПК-2.4
85.		Содержание заключения при аудите состояния информационной безопасности предприятия.	ОПК-5 ОПК-10 ОПК-2.4
86.		Назначение программных средства, реализующих методологии анализа рисков.	ОПК-5 ОПК-10 ОПК-2.4
87.		Опишите назначение и возможности семейства программных продуктов "CRAMM".	ОПК-5 ОПК-10 ОПК-2.4
88.		Перечислите программные средства, реализующие методологии анализа рисков.	ОПК-5 ОПК-10 ОПК-2.4

89.		Назначение и основные функции программных средств, интегрируемых в информационную систему предприятия.	ОПК-5 ОПК-10 ОПК-2.4
90.		Перечислите и охарактеризуйте известные программные средства, интегрируемые в информационную систему предприятия.	ОПК-5 ОПК-10 ОПК-2.4
91.		Дайте понятие инцидента в сфере информационной безопасности и причины его	ОПК-5 ОПК-10 ОПК-2.4
92.		Дайте характеристику этапа оценка и последующий анализ процесса нападения и его обстоятельств при реагировании на инциденты.	ОПК-5 ОПК-10 ОПК-2.4
93.		Оценка прямого и морального ущерба от произошедшего нарушения информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
94.		Устранение негативных последствий от инцидента в сфере информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
95.		Дайте характеристику услуги первичной постановки системы управления информационной безопасностью.	ОПК-5 ОПК-10 ОПК-2.4
96.		Дайте характеристику услуги администрирования информационных систем и средств защиты информации.	ОПК-5 ОПК-10 ОПК-2.4
97.		Дайте характеристику услуги создания инфраструктуры публичных ключей (Public Key Infrastructure, PKI).	ОПК-5 ОПК-10 ОПК-2.4
98.		Основные стадии процесса страхования информационных рисков.	ОПК-5 ОПК-10 ОПК-2.4
99.		Страхование в сфере информационной безопасности и основные объекты страхования.	ОПК-5 ОПК-10 ОПК-2.4

100.		Основные стадии процесса страхования информационных рисков.	ОПК-5 ОПК-10 ОПК-2.4
101.		Основные направления внешней организационной работы корпорации Microsoft в сфере информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
102.		Сущность методологии Жизненного цикла безопасной разработки – Microsoft Security Development Lifecycle (SDL).	ОПК-5 ОПК-10 ОПК-2.4
103.		Сущность программы построения партнерских отношений с различными независимыми компаниями Microsoft Security Partners.	ОПК-5 ОПК-10 ОПК-2.4
104.		Сущность программы обеспечения безопасности правительств Government Security Program (GSP).	ОПК-5 ОПК-10 ОПК-2.4
105.		Централизованная сертификация программных продуктов в государственных органах является для корпорации Microsoft.	ОПК-5 ОПК-10 ОПК-2.4
106.		Направления работы органов исполнительной власти в сфере информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
107.		Общая политика России в сфере информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
108.		Национальная политика (доктрина, национальный план, национальная стратегия) информационной безопасности.	ОПК-5 ОПК-10 ОПК-2.4
109.		Структура органов государственной власти, обеспечивающих информационную безопасность в РФ.	ОПК-5 ОПК-10 ОПК-2.4
110.	c)	Основными рисками информационной безопасности являются: a) искажение, уменьшение объема, перекодировка информации b) техническое вмешательство, выведение из строя оборудования сети	ОПК-5 ОПК-10 ОПК-2.4

		c) +: потеря, искажение, утечка информации d) навязанное шифрование информации с сокрытием ключа	
111.	a)	К основным функциям системы безопасности можно отнести все перечисленное: a) +: установление регламента, аудит системы, выявление рисков b) установка новых офисных приложений, смена хостинг-компании c) внедрение аутентификации, проверки контактных данных пользователей d) шифрование информации	ОПК-5 ОПК-10 ОПК-2.4
112.	a)	Принципом политики информационной безопасности является принцип … a) +: невозможности миновать защитные средства сети (системы) b) усиления основного звена сети, системы c) полного блокирования доступа при риск-ситуациях d) внедрение аутентификации, проверки контактных данных пользователей	ОПК-5 ОПК-10 ОПК-2.4
113.	a)	Что понимается под конфиденциальностью информации? a) +: известность ее содержания только имеющим соответствующие полномочия субъектам b) неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения c) способность обеспечения беспрепятственного доступа субъектов к интересующей их информации	ОПК-5 ОПК-10 ОПК-2.4

		d) способность обеспечения беспрепятственного раскрытия смысла передаваемой информации с помощью ключа	
114.	a)	Что понимается под целостностью информации? известность ее содержания только имеющим соответствующие полномочия субъектам a) +: неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения b) способность обеспечения беспрепятственного доступа субъектов к интересующей их информации c) способность обеспечения беспрепятственного раскрытия смысла передаваемой информации с помощью ключа	ОПК-5 ОПК-10 ОПК-2.4
115.	c)	Что понимается под доступностью информации? a) известность ее содержания только имеющим соответствующие полномочия субъектам b) неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения c) +: способность обеспечения беспрепятственного доступа субъектов к интересующей их информации d) способность обеспечения беспрепятственного раскрытия смысла передаваемой информации с помощью ключа	ОПК-5 ОПК-10 ОПК-2.4
116.	c)	Что понимается под угрозой безопасности информации? a) возникновение явления или события в форме хищения ключа шифрования данных телекоммуникационной системы b) возникновение явления или события в форме хищения ключа шифрования ключей телекоммуникационной системы	ОПК-5 ОПК-10 ОПК-2.4

		c) +: возникновение такого явления или события, следствием которого могут быть негативные воздействия на информацию: нарушение физической целостности, нарушение логической структуры, несанкционированная модификация, несанкционированное получение, несанкционированное размножение d) действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной её уязвимости	
117.	а)	Что называется основными техническими средствами и системами (ОТСС)? a) +: это технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации, средства и системы связи и передачи данных, включая коммуникационное оборудование, используемые для обработки и передачи конфиденциальной информации b) это технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации c) это средства и системы связи и передачи данных, включая коммуникационное оборудование, используемые для обработки и передачи конфиденциальной информации d) это технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации	ОПК-5 ОПК-10 ОПК-2.4

118.	d)	Что называется вспомогательными техническими средствами и системами (ВТСС)? a) это технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации b) это средства и системы связи и передачи данных, включая коммуникационное оборудование, используемые для обработки и передачи конфиденциальной информации c) это технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации d) +: это технические средства и системы, не предназначенные для передачи, обработки и хранения конфиденциальной информации, размещаемые совместно с основными техническими средствами и системами или в защищаемых помещениях	ОПК-5 ОПК-10 ОПК-2.4
119.	a)	Что называется контролируемой зоной? a) +: это территория (либо здание, группа помещений, помещение), на которой исключено неконтролируемое пребывание лиц и транспортных средств, не имеющих постоянного или разового допуска b) это территория (либо здание, группа помещений, помещение), на которой исключено неконтролируемое пребывание лиц и транспортных средств, имеющих постоянный или разовый допуск на них c) это территория (либо здание, группа помещений, помещение), которая определяется руководством организации	ОПК-5 ОПК-10 ОПК-2.4

		d) это территория (либо здание, группа помещений, помещение), которая определяется исходя из конкретной обстановки в месте расположения объекта и возможностей использования технических средств перехвата	
120.	c)	Сколько условных уровней используется для реализации политики безопасности предприятия: a) один b) два c) +: три d) четыре	ОПК-5 ОПК-10 ОПК-2.4
121.	a)	Как называется стандарт ГОСТ Р ИСО/МЭК 27001-2006, используемый для создания системы управления информационной безопасностью предприятия? a) +: Системы обеспечения информационной безопасности b) Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. c) Информационная технология. Практические правила управления информационной безопасностью. d) Информационная технология. Методы и средства обеспечения безопасности	ОПК-5 ОПК-10 ОПК-2.4
122.	a)	Перечислите знания и навыки, которыми должен обладать аудитор системы менеджмента информационной безопасности предприятия. a) +: существующие угрозы информационной безопасности, уязвимости, меры и средства контроля и управления;	ОПК-5 ОПК-10 ОПК-2.4

		организационные, правовые и договорные аспекты системы менеджмента информационной безопасности; общие знания информационной технологии и методов обеспечения информационной безопасности; методы менеджмента информационной безопасности. b) существующие угрозы информационной безопасности, уязвимости, меры и средства контроля и управления; организационные, правовые и договорные аспекты системы менеджмента информационной безопасности. c) общие знания информационной технологии и методов обеспечения информационной безопасности; методы менеджмента информационной безопасности. d) методы поиска угроз информационной безопасности. e) существующие угрозы информационной безопасности, уязвимости, меры и средства контроля и управления; организационные, правовые и договорные аспекты системы менеджмента информационной безопасности; общие знания информационной технологии и методов обеспечения информационной безопасности; методы менеджмента информационной безопасности; общие знания бизнес-процессов предприятия.	
123.	d)	Что входит в перечень ценных активов компании с точки зрения информационной безопасности? a) информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, научно-исследовательская информация, документация, обучающие материалы и пр.).	ОПК-5 ОПК-10 ОПК-2.4

		b) сервисы (поддерживающая инфраструктура); сотрудники компании, их квалификация и опыт; нематериальные ресурсы (репутация и имидж компании). c) программное обеспечение; материальные активы (компьютерное оборудование, средства телекоммуникаций и пр.). d) +: информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, научно-исследовательская информация, документация, обучающие материалы и пр.); сервисы (поддерживающая инфраструктура); сотрудники компании, их квалификация и опыт; нематериальные ресурсы (репутация и имидж компании); программное обеспечение; материальные активы (компьютерное оборудование, средства телекоммуникаций и пр.). e) информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, научно-исследовательская информация, документация, обучающие материалы и пр.); сервисы (поддерживающая инфраструктура); сотрудники компании, их квалификация и опыт; нематериальные ресурсы (репутация и имидж компании); программное обеспечение; материальные активы (компьютерное оборудование, средства телекоммуникаций и пр.); уставной капитал компании.	
124.	a)	Что входит в понятие «Управление информационной безопасностью организации»? (выберите несколько правильных ответов)	ОПК-5 ОПК-10 ОПК-2.4

		a) +: это управление персоналом, рисками, ресурсами, средствами защиты и т.п. b) +: это неотъемлемый элемент управления предприятием, который позволяет коллективно использовать конфиденциальную информацию, обеспечивая при этом ее защиту, а так же защиту вычислительных ресурсов. c) +: это циклический процесс, включающий: осознание степени необходимости защиты информации; сбор и анализ данных о состоянии информационной безопасности в организации; оценку информационных рисков; планирование мер по обработке рисков; реализацию и внедрение соответствующих механизмов контроля; распределение ролей и ответственности; обучение и мотивацию персонала; оперативную работу по осуществлению защитных мероприятий; мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия. d) это процесс оценки эффективности защиты информации в организации.	
125.	b)	Что входит в понятие «система управления информационной безопасностью» (СУИБ) организации в соответствии со стандартом ISO 27001? a) это элемент управления предприятием, который позволяет коллективно использовать конфиденциальную информацию, обеспечивая при этом ее защиту, а так же защиту вычислительных ресурсов.	ОПК-5 ОПК-10 ОПК-2.4

		b) +: это часть общей системы управления организации, основанная на оценке бизнес рисков, которая создает, реализует, эксплуатирует, осуществляет мониторинг, пересмотр, сопровождение и совершенствование информационной безопасности организации. c) это система оценки эффективности защиты информации в организации.	
126.	a)	Влияет ли на повышение доходности бизнеса компании в целом процедура ее сертификации на соответствие международным стандартам по информационной безопасности? a) +: да. b) нет. c) да, при условии высокой доходности бизнеса. d) да, при условии низкой доходности бизнеса.	ОПК-5 ОПК-10 ОПК-2.4
127.	b)	Что понимается под документом, определяющим перечень и характеристики основных (актуальных) угроз безопасности и уязвимостей при их обработке в информационной системе (ИС), которые должны учитываться в процессе организации защиты информации, проектировании и разработке систем защиты информации, проведении проверок (контроля) защищенности ИС? a) характеристика основных (актуальных) угроз безопасности ИС. b) +: модель угроз безопасности ИС. c) характеристика уязвимостей ИС. d) модель уязвимостей ИС.	ОПК-5 ОПК-10 ОПК-2.4

128.	a) b) c)	По каким основным причинам необходима стандартизация в области информационной безопасности (ИБ)? (выберите несколько правильных ответов) по причине имеющихся общих тенденций к стандартизации в различных сферах. a) +: по причине необходимости выработки единых требований по ИБ. b) +: по причине необходимости выработки единых подходов к решению проблем ИБ. c) +: по причине необходимости выработки единых качественных показателей для оценки безопасности информационной системы и средств защиты. d) по всем названным причинам.	ОПК-5 ОПК-10 ОПК-2.4
129.	a) b)	Какие существуют основные группы международных стандартов в области информационной безопасности (ИБ)? (выберите несколько правильных ответов) a) +: группа оценочных стандартов по ИБ. b) +: группа, включающая в себя так называемые спецификации, регламентирующие вопросы реализации и использования методов и средств защиты информации. c) группа стандартов, объединенная в так называемую «Оранжевую книгу». d) все названные группы.	ОПК-5 ОПК-10 ОПК-2.4

130.	c)	Приведите классы (подклассы) защищённости информационных систем в соответствии с «Оранжевой книгой» по мере роста защищённости информационной системы. a) Класс A — содержит единственный подкласс A1. Класс B — содержит подклассы B1, B2 и B3. Класс C — содержит подклассы C1 и C2. Класс D — содержит подкласс D1. b) Класс A — содержит единственный подкласс A1. Класс B — содержит подклассы B1 и B2. Класс C — содержит подклассы C1 и C2. Класс D — содержит подкласс D1. c) +: Класс D — содержит подкласс D1. Класс C — содержит подклассы C1 и C2. Класс B — содержит подклассы B1, B2 и B3. Класс A — содержит единственный подкласс A1. d) Класс D — содержит подкласс D1. Класс C — содержит подклассы C1 и C2. Класс B — содержит подклассы B1 и B2. Класс A — содержит единственный подкласс A1.	ОПК-5 ОПК-10 ОПК-2.4
131.	b)	Какой из перечисленных стандартов служит основой при оценке характеристик безопасности ИТ-продуктов или систем для их применения с заданным уровнем риска? a) Стандарт ISO/IEC 17799 «Практические правила управления информационной безопасностью». b) +: Стандарт ISO/IEC 15408 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» (т.н. «Общие критерии»). c) Стандарт ISO 27001 «Информационные технологии - Методы защиты - Системы менеджмента информационной безопасности – Требования».	ОПК-5 ОПК-10 ОПК-2.4

132.	c)	Какой из перечисленных стандартов определяет требования к средствам контроля безопасности, специально разработанные для нужд организации, или ее части? a) Стандарт ISO/IEC 17799 «Практические правила управления информационной безопасностью». b) Стандарт ISO/IEC 15408 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» (т.н. «Общие критерии»). c) +: Стандарт ISO 27001 «Информационные технологии - Методы защиты - Системы менеджмента информационной безопасности – Требования».	ОПК-5 ОПК-10 ОПК-2.4
133.	a)	Какие структурные элементы содержит стандарт ISO/IEC 15408 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» (т.н. «Общие критерии»)? a) +: Часть 1. Введение и общая модель. Часть 2. «Функциональные требования безопасности». Часть 3. «Требования доверия к безопасности». b) Часть 1. Введение и общая модель. Часть 2. «Требования доверия к безопасности». Часть 3. «Функциональные требования безопасности». c) Часть 1. Введение и общая модель. Часть 2. «Требования доверия к безопасности». d) Часть 1. Введение и общая модель. Часть 2. «Функциональные требования безопасности».	ОПК-5 ОПК-10 ОПК-2.4

134.	b)	Каким категориям пользователей адресован стандарт ISO/IEC 15408? a) потребителям и разработчикам информационных продуктов и систем. b) +: потребителям, разработчикам и оценщикам информационных продуктов и систем. c) разработчикам и оценщикам информационных продуктов и систем. d) потребителям и оценщикам информационных продуктов и систем.	ОПК-5 ОПК-10 ОПК-2.4
135.	b)	Что понимается под типовым набором требований для некоторой категории объекта оценки в соответствии с ISO/IEC 15408? a) Задание по безопасности. b) +: Профиль защиты. c) Характеристика объекта оценки. d) Задание на оценку объекта.	ОПК-5 ОПК-10 ОПК-2.4
136.	a)	Что понимается под документом, содержащим требования безопасности для конкретной разработки, выполнение которых обеспечивает достижение поставленных целей безопасности в соответствии с ISO/IEC 15408? a) +: Задание по безопасности. b) Профиль защиты. c) Характеристика объекта оценки. d) Задание на оценку объекта.	ОПК-5 ОПК-10 ОПК-2.4

137.	d)	Какие основные принципы управления информационной безопасностью декларируются стандартом ГОСТ Р ИСО/МЭК 27001-2006? a) Применение процессного подхода к управлению безопасностью и администрирования компьютерных систем. b) Применение PDCA – модели и управления доступом к системе. c) Применение администрирования компьютерных систем и вычислительных сетей и управление доступом к системе. d) +: Применение процессного подхода к управлению безопасностью и PDCA – модели.	ОПК-5 ОПК-10 ОПК-2.4
138.	b)	Укажите правильную последовательность этапов создания системы управления информационной безопасности (СУИБ) в соответствии со стандартом ГОСТ Р ИСО/МЭК 27001-2006. a) Разработка СУИБ → Внедрение и функционирование СУИБ → Поддержка и улучшение СУИБ. b) +: Разработка СУИБ → Внедрение и функционирование СУИБ → Проведение мониторинга и анализа СУИБ → Поддержка и улучшение СУИБ. c) Разработка СУИБ → Внедрение и функционирование СУИБ → Проведение мониторинга и анализа СУИБ. d) Разработка СУИБ → Проведение мониторинга и анализа СУИБ → Поддержка и улучшение СУИБ.	ОПК-5 ОПК-10 ОПК-2.4
139.	a)	Укажите правильную последовательность основных этапов разработки системы управления информационной безопасности (СУИБ).	ОПК-5 ОПК-10 ОПК-2.4

		a) +: инвентаризация активов → категорирование активов → оценка защищенности информационной системы → оценка информационных рисков → обработка информационных рисков (в том числе определение конкретных мер для защиты ценных активов) → внедрение выбранных мер обработки рисков → контроль выполнения и эффективности выбранных мер. b) оценка защищенности информационной системы → инвентаризация активов → категорирование активов → оценка информационных рисков → обработка информационных рисков (в том числе определение конкретных мер для защиты ценных активов) → внедрение выбранных мер обработки рисков → контроль выполнения и эффективности выбранных мер. c) категорирование активов → инвентаризация активов → оценка защищенности информационной системы → оценка информационных рисков → обработка информационных рисков (в том числе определение конкретных мер для защиты ценных активов) → внедрение выбранных мер обработки рисков → контроль выполнения и эффективности выбранных мер.	
140.	a) c) e) f)	Что относится к ценным активам компании с точки зрения информационной безопасности в соответствии со стандартом ISO 17799? (выберите несколько правильных ответов) a) +: информационные ресурсы (базы и файлы данных, контракты и соглашения, системная документация, научно-исследовательская информация, документация, обучающие материалы и пр.) и программное обеспечение. b) банковские реквизиты компании.	ОПК-5 ОПК-10 ОПК-2.4

		c) +: материальные активы (компьютерное оборудование, средства телекоммуникаций и пр.) и сервисы (поддерживающая инфраструктура). d) идентификационный номер налогоплательщика (ИНН) компании. e) +: сотрудники компании, их квалификация и опыт. f) +: нематериальные ресурсы (репутация и имидж компании).	
141.	b)	В чем заключается оценка информационных рисков компании? a) в определении сведений о критичности активов, а также применяемых средствах защиты информации. b) +: в определении сведений о критичности активов, а также вероятностей реализации уязвимостей. c) в определении сведений о существующих угрозах информационной безопасности, а также вероятностей реализации уязвимостей.	ОПК-5 ОПК-10 ОПК-2.4
142.	b)	По какой формуле проводится оценка информационных рисков R компании? a) R=D/P(V) где D - критичность актива (ущерб); P(V) - вероятность реализации уязвимости. b) +: R=D·P(V) где D - критичность актива (ущерб); P(V) - вероятность реализации уязвимости. c) R=D-P(V) где D - критичность актива (ущерб); P(V) - вероятность реализации уязвимости. d) R=D+P(V) где D - критичность актива (ущерб); P(V) - вероятность реализации уязвимости.	ОПК-5 ОПК-10 ОПК-2.4

143.	b)	Какой способ обработки рисков компании характеризуется полным устранением источника риска? a) принятие рисков; b) +: уклонение от рисков; c) передача рисков; d) снижение рисков.	ОПК-5 ОПК-10 ОПК-2.4
144.	a) b) c) d) f) g)	Укажите способы нарушения информационной безопасности информационных систем (выберите несколько правильных ответов) a) +: получение несанкционированного доступа к определенным сведениям или массивам данных, распространение которых ограничено, с целью их изучения, копирования, распространения, незаконного использования и т.п.; b) +: несанкционированное использование информационных ресурсов (ресурсов вычислительных и телекоммуникационных систем) с целью получения выгоды или нанесения ущерба c) +: несанкционированная злонамеренная модификация (изменение) данных; d) +: кража денежных средств в электронных платежных системах и системах "клиент-банк", а также кража бездокументарных ценных бумаг и иные формы незаконного присвоения имущественных прав e) +: вывод из строя (полный или частичный) программных и аппаратных средств обработки, передачи и хранения информации; f) +: осуществление атак типа "отказ в обслуживании" (DoS)	ОПК-5 ОПК-10 ОПК-2.4

		g) +: распространение вирусов и других вредоносных программ, осуществляющих различные негативные воздействия h) разработка вирусов и других вредоносных программ	
145.	a) b) c) e) f)	Что входит в направления защиты информации, используемые владельцами информационных ресурсов и информационных систем? (выберите несколько правильных ответов) a) +: ограничение и разграничение доступа b) +: информационное скрытие c) +: введение избыточной информации и использование избыточных информационных систем (средств хранения, обработки и передачи информации) d) наказание виновных за хищение информации e) +: использование методов надежного хранения, преобразования и передачи информации f) +: нормативно-административное побуждение и принуждение	ОПК-5 ОПК-10 ОПК-2.4
146.	a) b) d) e)	Основные задачи организационно-управленческой деятельности (менеджмента) в сфере информационной безопасности (выберите несколько правильных ответов) обеспечение информационной системы криптографическими средствами a) +: обеспечение комплексности всех решений, реализуемых в процессе обеспечения информационной безопасности b) +: обеспечение непрерывности и целостности процессов информационной безопасности c) обеспечение информационной системы средствами инженерно-технической защиты информации	ОПК-5 ОПК-10 ОПК-2.4

		d) +: решение методических задач, лежащих в основе эффективного управления информационной безопасностью, таких, как вопросы управления рисками, экономическое моделирование и т.п. e) +: управление человеческими ресурсами и поведением персонала с учетом необходимости решения задач информационной безопасности	
147.	a)	Что предполагает непрерывность процессов обеспечения информационной безопасности? a) +: выделение необходимых ресурсов и организацию выполнения необходимых функций по защите информации в течение всего времени функционирования информационных систем и выполнения бизнес-функций b) взаимоувязанное выявление всех значимых информационных объектов, а также существующих и потенциально возможных угроз c) исчерпывающий анализ всех информационных ресурсов и всех возможных сценариев нападения на них и последующий подбор наиболее подходящих средств защиты d) отбор и допуск персонала для работы с определенными информационными ресурсами, обучение, контроль правильности выполнения обязанностей, создание необходимых условий для работы и т.п.	ОПК-5 ОПК-10 ОПК-2.4
148.	b)	Что предполагает комплексность решения задач информационной безопасности?	ОПК-5 ОПК-10 ОПК-2.4

		a) выделение необходимых ресурсов и организацию выполнения необходимых функций по защите информации в течение всего времени функционирования информационных систем и выполнения бизнес-функций b) +: взаимоувязанное выявление всех значимых информационных объектов, а также существующих и потенциально возможных угроз c) исчерпывающий анализ всех информационных ресурсов и всех возможных сценариев нападения на них и последующий подбор наиболее подходящих средств защиты d) отбор и допуск персонала для работы с определенными информационными ресурсами, обучение, контроль правильности выполнения обязанностей, создание необходимых условий для работы и т.п.	
149.	d)	Что предполагает управление человеческими ресурсами в рамках управления информационной безопасностью? a) выделение необходимых ресурсов и организацию выполнения необходимых функций по защите информации в течение всего времени функционирования информационных систем и выполнения бизнес-функций b) взаимоувязанное выявление всех значимых информационных объектов, а также существующих и потенциально возможных угроз c) исчерпывающий анализ всех информационных ресурсов и всех возможных сценариев нападения на них и последующий подбор наиболее подходящих средств защиты	ОПК-5 ОПК-10 ОПК-2.4

		d) +: отбор и допуск персонала для работы с определенными информационными ресурсами, обучение, контроль правильности выполнения обязанностей, создание необходимых условий для работы и т.п.	
150.	a)	Укажите правильную иерархию уровней организационной работы в сфере информационной безопасности a) +: организации-владельцы информационных ресурсов → уровень государственных организаций → уровень крупных международных ИТ-компаний → уровень международных организаций по стандартизации b) уровень международных организаций по стандартизации → уровень крупных международных ИТ-компаний → государственных организаций → организации-владельцы информационных ресурсов c) государственных организаций → организации-владельцы информационных ресурсов → уровень международных организаций по стандартизации → уровень крупных международных ИТ-компаний d) организации-владельцы информационных ресурсов → уровень крупных международных ИТ-компаний → уровень международных организаций по стандартизации → уровень государства	ОПК-5 ОПК-10 ОПК-2.4
151.	b)	Укажите специфичные методы организационной работы глобальных ИТ-компаний в сфере информационной безопасности	ОПК-5 ОПК-10 ОПК-2.4

		a) координация работы специалистов, экспертов и исследователей, представляющих различные заинтересованные стороны b) +: гибкое взаимодействие с клиентами (пользователями продуктов и услуг) с целью повышения эффективности использования информационных систем и получения отзывов для дальнейшего повышения качества поставляемых продуктов и услуг c) разработка национальных и международных правил (законов, конвенций, соглашений и т.п.), регулирующих отношения в информационной сфере; осуществление контроля (в различных формах); осуществление правоприменительной и правоохранительной деятельности d) выделение подразделений и специалистов, отвечающих за ИБ; разработка и применение внутренних политик и правил безопасности	
152.	c)	Укажите специфичные методы организационной работы государственных организаций в сфере информационной безопасности a) координация работы специалистов, экспертов и исследователей, представляющих различные заинтересованные стороны b) гибкое взаимодействие с клиентами (пользователями продуктов и услуг) с целью повышения эффективности использования информационных систем и получения отзывов для дальнейшего повышения качества поставляемых продуктов и услуг c) +: разработка национальных и международных правил (законов, конвенций, соглашений и т.п.), регулирующих отношения в информационной сфере; осуществление контроля (в различных	ОПК-5 ОПК-10 ОПК-2.4

		формах); осуществление правоприменительной и правоохранительной деятельности d) выделение подразделений и специалистов, отвечающих за ИБ; разработка и применение внутренних политик и правил безопасности	
153.	d)	Укажите специфичные методы организационной работы пользователей информационных систем – владельцев информации в сфере информационной безопасности a) координация работы специалистов, экспертов и исследователей, представляющих различные заинтересованные стороны b) гибкое взаимодействие с клиентами (пользователями продуктов и услуг) с целью повышения эффективности использования информационных систем и получения отзывов для дальнейшего повышения качества поставляемых продуктов и услуг c) разработка национальных и международных правил (законов, конвенций, соглашений и т.п.), регулирующих отношения в информационной сфере; осуществление контроля (в различных формах); осуществление правоприменительной и правоохранительной деятельности d) +: выделение подразделений и специалистов, отвечающих за ИБ; разработка и применение внутренних политик и правил безопасности	ОПК-5 ОПК-10 ОПК-2.4
154.	a)	Укажите правильную последовательность выполнения основных этапов разработки СУИБ a) +: инвентаризация активов → категорирование активов → оценка защищенности информационной системы → оценка	ОПК-5 ОПК-10 ОПК-2.4

		информационных рисков → обработка информационных рисков (в том числе определение конкретных мер для защиты ценных активов) → внедрение выбранных мер обработки рисков → контроль выполнения и эффективности выбранных мер b) инвентаризация активов → категорирование активов → оценка защищенности информационной системы → оценка информационных рисков → внедрение выбранных мер обработки рисков → контроль выполнения и эффективности выбранных мер → обработка информационных рисков (в том числе определение конкретных мер для защиты ценных активов) c) категорирование активов → инвентаризация активов → оценка защищенности информационной системы → оценка информационных рисков → обработка информационных рисков (в том числе определение конкретных мер для защиты ценных активов) → внедрение выбранных мер обработки рисков → контроль выполнения и эффективности выбранных мер d) инвентаризация активов → категорирование активов → оценка информационных рисков → обработка информационных рисков (в том числе определение конкретных мер для защиты ценных активов) → оценка защищенности информационной системы → внедрение выбранных мер обработки рисков → контроль выполнения и эффективности выбранных мер	
155.	a)	Что понимается под категорированием активов компании как этапа разработки системы управления информационной безопасностью? a) +: оценка критичности активов компании для бизнес-процессов компании или определение ущерба компании в случае нарушения информационной безопасности активов	ОПК-5 ОПК-10 ОПК-2.4

		b) определение активов компании с точки зрения информационной безопасности c) определение угроз, действующих на активы, а также уязвимости информационной системы, в которой обрабатываются активы и которые могут привести к реализации угроз d) расчет информационных рисков, который выполняется с учетом сведений о критичности активов, а также вероятностей реализации уязвимостей e) определение действий по отношению к рискам, которые требуется выполнить в компании f) выполнение процедуры и регулярном контроле её выполнения, а также оценки ее эффективности, внесении корректирующих и превентивных действий g) выполнение процедуры постоянного контроля и анализа	
156.	b)	Что понимается под инвентаризацией активов компании как этапа разработки системы управления информационной безопасностью? a) оценка критичности активов компании для бизнес-процессов компании или определение ущерба компании в случае нарушения информационной безопасности активов b) +: определение активов компании с точки зрения информационной безопасности c) определение угроз, действующих на активы, а также уязвимости информационной системы, в которой обрабатываются активы и которые могут привести к реализации угроз d) расчет информационных рисков, который выполняется с учетом сведений о критичности активов, а также вероятностей реализации уязвимостей	ОПК-5 ОПК-10 ОПК-2.4

		e) определение действий по отношению к рискам, которые требуется выполнить в компании f) выполнение процедуры и регулярном контроле её выполнения, а также оценки ее эффективности, внесении корректирующих и превентивных действий g) выполнение процедуры постоянного контроля и анализа	
157.	c)	Что понимается под оценкой защищенности информационной системы компании как этапа разработки системы управления информационной безопасностью? a) оценка критичности активов компании для бизнес-процессов компании или определение ущерба компании в случае нарушения информационной безопасности активов b) определение активов компании с точки зрения информационной безопасности c) +: определение угроз, действующих на активы, а также уязвимости информационной системы, в которой обрабатываются активы и которые могут привести к реализации угроз d) расчет информационных рисков, который выполняется с учетом сведений о критичности активов, а также вероятностей реализации уязвимостей e) определение действий по отношению к рискам, которые требуется выполнить в компании f) выполнение процедуры и регулярном контроле её выполнения, а также оценки ее эффективности, внесении корректирующих и превентивных действий g) выполнение процедуры постоянного контроля и анализа	ОПК-5 ОПК-10 ОПК-2.4

158.	d)	Что понимается под оценкой информационных рисков компании как этапа разработки системы управления информационной безопасностью? a) оценка критичности активов компании для бизнес-процессов компании или определение ущерба компании в случае нарушения информационной безопасности активов b) определение активов компании с точки зрения информационной безопасности c) определение угроз, действующих на активы, а также уязвимости информационной системы, в которой обрабатываются активы и которые могут привести к реализации угроз d) +: расчет информационных рисков, который выполняется с учетом сведений о критичности активов, а также вероятностей реализации уязвимостей e) определение действий по отношению к рискам, которые требуется выполнить в компании f) выполнение процедуры и регулярном контроле её выполнения, а также оценки ее эффективности, внесении корректирующих и превентивных действий g) выполнение процедуры постоянного контроля и анализа	ОПК-5 ОПК-10 ОПК-2.4
159.	e)	Что понимается под обработкой информационных рисков компании как этапа разработки системы управления информационной безопасностью? a) оценка критичности активов компании для бизнес-процессов компании или определение ущерба компании в случае нарушения информационной безопасности активов	ОПК-5 ОПК-10 ОПК-2.4

		b) определение активов компании с точки зрения информационной безопасности c) определение угроз, действующих на активы, а также уязвимости информационной системы, в которой обрабатываются активы и которые могут привести к реализации угроз d) расчет информационных рисков, который выполняется с учетом сведений о критичности активов, а также вероятностей реализации уязвимостей e) +: определение действий по отношению к рискам, которые требуется выполнить в компании f) выполнение процедуры и регулярном контроле её выполнения, а также оценки ее эффективности, внесении корректирующих и превентивных действий g) выполнение процедуры постоянного контроля и анализа	
160.	f)	Что понимается под внедрением выбранных мер обработки рисков компании как этапа разработки системы управления информационной безопасностью? a) оценка критичности активов компании для бизнес-процессов компании или определение ущерба компании в случае нарушения информационной безопасности активов b) определение активов компании с точки зрения информационной безопасности c) определение угроз, действующих на активы, а также уязвимости информационной системы, в которой обрабатываются активы и которые могут привести к реализации угроз	ОПК-5 ОПК-10 ОПК-2.4

		d) расчет информационных рисков, который выполняется с учетом сведений о критичности активов, а также вероятностей реализации уязвимостей e) определение действий по отношению к рискам, которые требуется выполнить в компании f) +: выполнение процедуры и регулярном контроле её выполнения, а также оценки ее эффективности, внесении корректирующих и превентивных действий g) выполнение процедуры постоянного контроля и анализа	
161.	a) b) d) e) g) h)	Укажите обязательные этапы работ по обеспечению режима информационной безопасности (ИБ) информационной системы (выберите несколько правильных ответов) a) +: определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания b) +: оценка рисков c) исключение рисков d) +: выбор контрмер, обеспечивающих режим ИБ e) +: управление рисками f) исключение угроз ИБ g) +: аудит системы управления ИБ h) +: выработка политики безопасности	ОПК-5 ОПК-10 ОПК-2.4
162.	b)	Сколько этапов включает процесс определения политики безопасности предприятия? a) пять b) +: шесть	ОПК-5 ОПК-10 ОПК-2.4

		c) семь d) восемь	
163.	а)	Является или нет разработка концепции и политики информационной безопасности компании функцией отдела информационной безопасности компании? a) +: является b) не является c) является, в случае необходимости разработки политики информационной безопасности компании	ОПК-5 ОПК-10 ОПК-2.4
164.	а)	Является или нет выработка принципов классификации информационных активов компании и оценивания их защищенности функцией отдела информационной безопасности компании? a) +: является b) не является c) является, в случае необходимости проведения классификации информационных активов компании и оценивания их защищенности	ОПК-5 ОПК-10 ОПК-2.4
165.	а)	Чем является информационное обеспечение руководства компании регулярными обзорами и аналитическими справками о текущем состоянии информационной безопасности компании, выдержками о результатах проверки выполнения политики безопасности? a) +: функцией отдела информационной безопасности компании b) функцией отдела автоматизации компании c) функцией отдела контроля качества продукции компании d) функцией отдела производства компании	ОПК-5 ОПК-10 ОПК-2.4

166.	a)	Перечислите в правильной последовательности этапы жизненного цикла систем защиты информации (СЗИ) a) +: определение требований к проектированию СЗИ; эксплуатация СЗИ; сопровождение СЗИ; парирование инцидентов b) эксплуатация СЗИ; сопровождение СЗИ; парирование инцидентов c) определение требований к проектированию СЗИ; сопровождение СЗИ; эксплуатация СЗИ; парирование инцидентов d) определение требований к проектированию СЗИ; эксплуатация СЗИ; сопровождение СЗИ; парирование инцидентов; внесение изменений в функции, выполняемые СЗИ	ОПК-5 ОПК-10 ОПК-2.4
167.	b)	Сколько шагов включает процесс анализа информационных рисков предприятия? a) три b) +: четыре c) пять d) шесть	ОПК-5 ОПК-10 ОПК-2.4
168.	a) b) c) d)	Какие процессы включает в себя процедура анализа информационных рисков предприятия? (выберите несколько правильных ответов) a) +: идентификация и количественная оценка информационных ресурсов компании, значимых для бизнеса b) +: оценивание возможных угроз c) +: оценивание существующих уязвимостей	ОПК-5 ОПК-10 ОПК-2.4

		d) +: оценивание эффективности средств обеспечения информационной безопасности e) принятие решение по риску	
169.	a)	Входит или нет процесс оценивания существующих уязвимостей в процедуру анализа информационных рисков предприятия? a) +: входит b) не входит c) входит, в случае необходимости его проведения	ОПК-5 ОПК-10 ОПК-2.4
170.	a)	Входит или нет процесс оценивания возможных угроз в процедуру анализа информационных рисков предприятия? a) +: входит b) не входит c) входит, в случае необходимости его проведения	ОПК-5 ОПК-10 ОПК-2.4
171.	a)	Входит или нет процесс оценивания эффективности средств обеспечения информационной безопасности в процедуру анализа информационных рисков предприятия? a) +: входит b) не входит c) входит, в случае необходимости его проведения	ОПК-5 ОПК-10 ОПК-2.4
172.	a)	Входит или нет процесс идентификации и количественной оценки информационных ресурсов компании, значимых для бизнеса, в процедуру анализа информационных рисков предприятия? a) +: входит	ОПК-5 ОПК-10 ОПК-2.4

		b) не входит c) входит, в случае необходимости его проведения	
173.	b)	Входит или нет процесс принятия решение по риску в процедуру анализа информационных рисков предприятия? a) входит b) +: не входит c) входит, в случае необходимости его проведения	ОПК-5 ОПК-10 ОПК-2.4
174.	b)	Сколько уровней входит в состав политики информационной безопасности на предприятии? a) два b) +: три c) четыре	ОПК-5 ОПК-10 ОПК-2.4
175.	c)	К какому уровню относится политика безопасности, охватывающая отдельные элементы информационных систем и участки обработки и хранения информации и описывает конкретные процедуры и документы, связанные с обеспечением информационной безопасности? a) к политике безопасности верхнего уровня b) к политике безопасности среднего уровня c) +: к политике безопасности нижнего уровня	ОПК-5 ОПК-10 ОПК-2.4
176.	a)	К какому уровню относится политика безопасности, определяющая основу для разработки индивидуальных политик безопасности (на более низких уровнях), правил и инструкций, регулирующих отдельные вопросы?	ОПК-5 ОПК-10 ОПК-2.4

		a) +: к политике безопасности верхнего уровня b) к политике безопасности среднего уровня c) к политике безопасности нижнего уровня	
177.	b) c) d)	Что обязательно входит в общие правила разработки политик безопасности? (выберите несколько правильных ответов) a) текст политики безопасности должен содержать перечень средств защиты информации, используемых на предприятии b) +: политики безопасности на более низких уровнях должны полностью подчиняться соответствующей политике верхнего уровня, а также действующему законодательству и требованиям государственных органов c) +: текст политики безопасности должен содержать только четкие и однозначные формулировки, не допускающие двойного толкования d) +: текст политики безопасности должен быть доступен для понимания тех сотрудников, которым он адресован e) текст политики безопасности должен содержать перечень должностных лиц предприятия, ответственных за обеспечение информационной безопасности	ОПК-5 ОПК-10 ОПК-2.4
178.	a)	Укажите правильную последовательность основных этапов общего жизненного цикла политики информационной безопасности. a) +: проведение предварительного исследования состояния информационной безопасности → разработка политики безопасности → внедрение разработанной политики безопасности → анализ соблюдения требований внедренной	ОПК-5 ОПК-10 ОПК-2.4

		политики безопасности и формулирование требований по ее дальнейшему совершенствованию b) разработка политики безопасности → внедрение разработанной политики безопасности → анализ соблюдения требований внедренной политики безопасности и формулирование требований по ее дальнейшему совершенствованию c) проведение предварительного исследования состояния информационной безопасности → разработка политики безопасности → внедрение разработанной политики безопасности d) проведение предварительного исследования состояния информационной безопасности → составление плана действий по разработке политики безопасности → разработка политики безопасности → внедрение разработанной политики безопасности → анализ соблюдения требований внедренной политики безопасности и формулирование требований по ее дальнейшему совершенствованию	
179.	c)	Что понимается под аудитом состояния информационной безопасности на предприятии? a) определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания b) оценка информационных рисков предприятия c) +: экспертное обследование основных аспектов информационной безопасности предприятия и их проверка на соответствие определенным требованиям d) разработка политики безопасности предприятия	ОПК-5 ОПК-10 ОПК-2.4

180.	a)	Укажите основные виды аудита информационной безопасности предприятия в зависимости от того, кто его осуществляет (выберите несколько правильных ответов) a) +: внешний b) периодический c) внеплановый	ОПК-5 ОПК-10 ОПК-2.4
181.	a) b) c) d) f)	Что относится к целям аудита информационной безопасности предприятия? (выберите несколько правильных ответов) a) +: установление степени защищенности информационных ресурсов предприятия, выявление недостатков и определение направлений дальнейшего развития системы защиты информации b) +: проверка руководством предприятия и другими заинтересованными лицами достижения поставленных целей в сфере информационной безопасности, выполнения требований политики безопасности c) +: сертификация на соответствие общепризнанным нормам и требованиям в сфере информационной безопасности (в частности, на соответствие национальным и международным стандартам) d) определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания e) оценка информационных рисков предприятия	ОПК-5 ОПК-10 ОПК-2.4

		f) +: контроль эффективности вложений в приобретение средств защиты информации и реализацию мероприятий по обеспечению информационной безопасности	
182.	c)	Укажите стратегическую задачу, решаемую при аудите информационной безопасности предприятия a) определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания b) оценка информационных рисков предприятия c) +: демонстрация надежности предприятия, его способности выступать в качестве устойчивого партнера, способного обеспечить комплексную защиту информационных ресурсов d) сертификация на соответствие общепризнанным нормам и требованиям в сфере информационной безопасности (в частности, на соответствие национальным и международным стандартам)	ОПК-5 ОПК-10 ОПК-2.4
183.	a) c)	Укажите причины проведения внешнего аудита информационной безопасности предприятия (выберите несколько правильных ответов) a) +: повышения объективности, независимости и профессионального уровня проверки b) демонстрация надежности предприятия, его способности выступать в качестве устойчивого партнера, способного обеспечить комплексную защиту информационных ресурсов c) +: получения заключений о состоянии информационной безопасности и соответствии международным стандартам от независимых аудиторов	ОПК-5 ОПК-10 ОПК-2.4

184.	a) b) c)	Каким требованиям должна отвечать организация, осуществляющая внешний аудит? (выберите несколько правильных ответов) a) +: иметь право (лицензию) на выдачу заключений о соответствии определенным требованиям (например, аккредитацию UKAS – United Kingdom Accreditation Service) b) +: сотрудники должны иметь право доступа к информации, составляющей государственную тайну (если такая информация имеется на проверяемом предприятии) c) +: обладать необходимыми программными и аппаратными средствами для исчерпывающей проверки имеющегося у предприятия программного и аппаратного обеспечения d) иметь возможность осуществлять экспертное обследование основных аспектов информационной безопасности предприятия и их проверку на соответствие требованиям информационной безопасности	ОПК-5 ОПК-10 ОПК-2.4
185.	a) b) e) f)	Перечислите основные этапы проведения аудита информационной безопасности предприятия (выберите несколько правильных ответов) a) +: инициирование проведения аудита b) +: непосредственно осуществление сбора информации и проведение обследования аудиторами c) определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания d) оценка информационных рисков предприятия e) +: анализ собранных данных и выработка рекомендаций	ОПК-5 ОПК-10 ОПК-2.4

		f) +: подготовка аудиторского отчета и аттестационного заключения	
186.	b)	К какой стадии аудита информационной безопасности предприятия относится процедура анализа имеющейся политики информационной безопасности предприятия и другой организационной документации? a) инициирование проведения аудита b) +: непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	ОПК-5 ОПК-10 ОПК-2.4
187.	a)	К какой стадии аудита информационной безопасности предприятия относится процедура определения основных угроз, средства защиты от которых необходимо подвергнуть аудиту? a) +: инициирование проведения аудита b) непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	ОПК-5 ОПК-10 ОПК-2.4
188.	a)	К какой стадии аудита информационной безопасности предприятия относится процедура определения перечня обследуемых информационных ресурсов и информационных систем (подсистем)? a) +: инициирование проведения аудита b) непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций	ОПК-5 ОПК-10 ОПК-2.4

		d) подготовка аудиторского отчета и аттестационного заключения	
189.	a)	К какой стадии аудита информационной безопасности предприятия относится процедура определения перечня элементов системы обеспечения информационной безопасности, которые необходимо включить в процесс проверки (организационное, правовое, программно-техническое, аппаратное обеспечение)? a) +: инициирование проведения аудита b) непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	ОПК-5 ОПК-10 ОПК-2.4
190.	a)	К какой стадии аудита информационной безопасности предприятия относится процедура определения перечня зданий, помещений и территорий, в пределах которых будет проводиться аудит? a) +: инициирование проведения аудита b) непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	ОПК-5 ОПК-10 ОПК-2.4
191.	b)	К какой стадии аудита информационной безопасности предприятия относится процедура проведения совещаний, опросов, доверительных бесед и интервью с сотрудниками предприятия? a) инициирование проведения аудита b) +: непосредственно осуществление сбора информации и проведение обследования аудиторами	ОПК-5 ОПК-10 ОПК-2.4

		c) анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	
192.	b)	К какой стадии аудита информационной безопасности предприятия относится процедура проверки состояния физической безопасности информационной инфраструктуры предприятия? a) инициирование проведения аудита b) +: непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	ОПК-5 ОПК-10 ОПК-2.4
193.	b)	К какой стадии аудита информационной безопасности предприятия относится процедура технического обследования информационных систем – программных и аппаратных средств (инструментальная проверка защищенности)? a) инициирование проведения аудита b) +: непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	ОПК-5 ОПК-10 ОПК-2.4
194.	d)	К какой стадии аудита информационной безопасности предприятия относится процедура подготовки заключения о практическом выполнении требований, предусмотренных политикой информационной безопасности предприятия и иными требованиями и документами? a) инициирование проведения аудита	ОПК-5 ОПК-10 ОПК-2.4

		b) непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций d) +: подготовка аудиторского отчета и аттестационного заключения	
195.	d)	К какой стадии аудита информационной безопасности предприятия относится процедура подготовки заключения о степени соответствия фактического уровня информационной безопасности требованиям определенных стандартов и нормативных документов? a) инициирование проведения аудита b) непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций d) +: подготовка аудиторского отчета и аттестационного заключения	ОПК-5 ОПК-10 ОПК-2.4
196.	c)	К какой стадии аудита информационной безопасности предприятия относится процедура описание причинно-следственных взаимосвязей между выявленными особенностями функционирования предприятия и увеличением рисков нарушения информационной безопасности? a) инициирование проведения аудита b) непосредственно осуществление сбора информации и проведение обследования аудиторами c) +: анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	ОПК-5 ОПК-10 ОПК-2.4

197.	c)	К какой стадии аудита информационной безопасности предприятия относится процедура выявления конкретных особенностей программных и аппаратных средств, бизнес-процедур, организационных правил и распределений функциональных обязанностей и полномочий, которые могут негативно повлиять на обеспечение информационной безопасности? a) инициирование проведения аудита b) непосредственно осуществление сбора информации и проведение обследования аудиторами c) +: анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	ОПК-5 ОПК-10 ОПК-2.4
198.	b)	К какой стадии аудита информационной безопасности предприятия относится процедура организации процесса обучения пользователей приемам и правилам безопасного использования информационных систем? a) инициирование проведения аудита b) +: непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	ОПК-5 ОПК-10 ОПК-2.4
199.	d)	К какой стадии аудита информационной безопасности предприятия относится процедура оценки состояния (уровня) защищенности информационных ресурсов и информационных систем? a) инициирование проведения аудита b) непосредственно осуществление сбора информации и проведение обследования аудиторами	ОПК-5 ОПК-10 ОПК-2.4

		c) анализ собранных данных и выработка рекомендаций d) +: подготовка аудиторского отчета и аттестационного заключения	
200.	b)	К какой стадии аудита информационной безопасности предприятия относится процедура организации процесса обучения пользователей приемам и правилам безопасного использования информационных систем? a) инициирование проведения аудита b) +: непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	ОПК-5 ОПК-10 ОПК-2.4
201.	b)	К какой стадии аудита информационной безопасности предприятия относится процедура организации процессов повышения квалификации администраторов информационных систем и систем защиты информации? a) инициирование проведения аудита b) +: непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	ОПК-5 ОПК-10 ОПК-2.4
202.	b)	К какой стадии аудита информационной безопасности предприятия относится процедура организации процессов организации работ и координации действий при выявлении нарушений информационной	ОПК-5 ОПК-10 ОПК-2.4

		безопасности и восстановлении работы информационных систем после сбоев и нападений? a) инициирование проведения аудита b) +: непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	
203.	a) b) c)	Какие вопросы рассматриваются при анализе политики информационной безопасности предприятия? (выберите несколько правильных ответов) a) +: полнота и глубина охвата всех вопросов, а также соответствие содержания политик нижнего уровня целям и задачам, установленным в политиках верхнего уровня b) +: понятность текста политики для людей, не являющихся техническими специалистами, а также четкость формулировок и невозможность их двойного толкования c) +: актуальность всех положений и требований политики, своевременность учета всех изменений, происходящих в информационных системах и бизнес-процессах d) определение сферы (границ) системы управления информационной безопасностью и конкретизация целей ее создания e) оценка информационных рисков предприятия	ОПК-5 ОПК-10 ОПК-2.4
204.	b)	Что понимается под каким-либо отклонением от нормального процесса использования информационных ресурсов и функционирования информационных систем, повлекшее ущерб для	ОПК-5 ОПК-10 ОПК-2.4

		определенных информационных активов предприятия или непосредственно создающее угрозу нанесения такого ущерба? a) угроза b) +: инцидент c) атака d) кража	
205.	a) b) c) d)	Какие основные этапы входят в процесс реагирования на инциденты? (выберите несколько правильных ответов) a) +: обнаружение нападения b) +: локализация нападения c) +: идентификация нападающих d) +: оценка и последующий анализ процесса нападения и его обстоятельств e) анализ собранных данных и выработка рекомендаций	ОПК-5 ОПК-10 ОПК-2.4
206.	a)	Каким образом реализуется этап реагирования на инциденты «обнаружение нападения»? a) +: использованием специальных программных и иногда аппаратных средств b) определением конкретных параметров нарушения c) блокированием (полным или частичным) работы информационной системы d) резким нехарактерным повышением нагрузки на информационные системы или её отдельные элементы	ОПК-5 ОПК-10 ОПК-2.4

207.	a) b) c)	Перечислите косвенные свидетельства прекращения функционирования отдельных элементов информационных систем (выберите несколько правильных ответов) a) +: использование информационных систем и определенных учетных записей в нехарактерное время (рано утром, поздно вечером и т.п.) b) +: резкое нехарактерное повышение нагрузки на информационные системы или их отдельные элементы (сегменты сети, хранилища данных и т.п.) c) +: изменение характера поведения пользователей (например, последовательности определенных действий при использовании информационной системы) d) полное блокирование работы информационной системы	ОПК-5 ОПК-10 ОПК-2.4
208.	a) b) c)	Какими характеристиками описывается процесс идентификации нападающего при реагировании на инцидент (выберите несколько правильных ответов) a) +: детальным изучением всех технических аспектов нападения b) +: проведением качественного анализа процесса нападения в контексте функционирования атакуемой системы защиты информации c) +: организацией взаимодействия со сторонними организациями, которые могут содействовать в идентификации нападающего d) использованием информационных систем и определенных учетных записей в нехарактерное время (рано утром, поздно вечером и т.п.) e) полным блокированием работы информационной системы	ОПК-5 ОПК-10 ОПК-2.4

209.	b) d) e) f)	Какие этапы входят в процесс оценки и анализа нападения и его обстоятельств при реагировании на инцидент (выберите несколько правильных ответов) a) детальное изучение всех технических аспектов нападения b) +: анализ целей и мотивов нападавших c) определение конкретных параметров нарушения d) +: анализ фундаментальных (организационных и технических) причин, которые сделали нападение возможным и успешным (если оно было успешным) e) +: анализ последствий (в том числе и долгосрочных) нападения для всей деятельности предприятия f) +: анализ и оценка работы персонала и взаимоотношений с предприятиями-партнерами	ОПК-5 ОПК-10 ОПК-2.4
210.	c) d) e)	Что входит в количественную экономическую оценку в форме прямого ущерба при инциденте в сфере информационной безопасности? (выберите несколько правильных ответов) a) затраты на приобретение новых средств защиты информации b) затраты на переподготовку сотрудников службы информационной безопасности c) +: затраты на восстановление утраченной информации d) +: затраты на замену скомпрометированных паролей, кодов и ключей e) +: стоимость поврежденного оборудования, штрафные санкции за разглашение конфиденциальной информации f) ущерб от непосредственного прекращения (приостановки, замедления) текущих операций предприятия	ОПК-5 ОПК-10 ОПК-2.4

		g) ущерб от негативного влияния возникшей внештатной ситуации на имидж компании h) величина падения рыночной стоимости предприятия	
211.	f) g) h)	Что входит в количественную экономическую оценку упущенной выгоды компании при инциденте в сфере информационной безопасности? (выберите несколько правильных ответов) a) затраты на приобретение новых средств защиты информации b) затраты на переподготовку сотрудников службы информационной безопасности c) затраты на восстановление утраченной информации d) затраты на замену скомпрометированных паролей, кодов и ключей e) стоимость поврежденного оборудования, штрафные санкции за разглашение конфиденциальной информации f) +: ущерб от непосредственного прекращения (приостановки, замедления) текущих операций предприятия g) +: ущерб от негативного влияния возникшей внештатной ситуации на имидж компании h) +: величина падения рыночной стоимости предприятия	ОПК-5 ОПК-10 ОПК-2.4
212.	a) b) e) f)	Что включает в себя процесс устранения негативных последствий нападения при инциденте в сфере информационной безопасности? (выберите несколько правильных ответов) a) +: смену скомпрометированных паролей отдельных пользователей b) +: переустановку поврежденных операционных систем, а также поврежденного программного обеспечения	ОПК-5 ОПК-10 ОПК-2.4

		c) приобретение новых средств защиты информации d) переподготовку сотрудников службы информационной безопасности e) +: восстановление нарушенной конфигурации (настроек) программного обеспечения и операционных систем f) +: восстановление поврежденной информации (баз данных, файлов), как из ранее созданных резервных копий, так и другими способами	
213.	a) b) c)	Что включается в основные задачи проверок защищенности и надежности отдельных элементов информационной инфраструктуры? (выберите несколько правильных ответов) a) +: оценка эффективности используемых технических (программных и аппаратных) средств защиты информации; b) +: оценка эффективности работы специалистов, ответственных за реагирование на инциденты; c) +: контроль соблюдения сотрудниками предприятия требований политики безопасности d) оценка средств защиты информации e) оценка уровня подготовки сотрудников службы информационной безопасности	ОПК-5 ОПК-10 ОПК-2.4
214.	a) b) c)	Какие из перечисленных стандартов относятся к группе управления информационной безопасностью? (выберите несколько правильных ответов) a) +: рекомендации X.800, «Архитектура безопасности для взаимодействия открытых систем» – регламентирует методы и средства обеспечения ИБ в компьютерных сетях;	ОПК-5 ОПК-10 ОПК-2.4

		b) +: международный стандарт ISO/IEC 17799 «Практические правила управления информационной безопасностью», разработанный на основе одноименного британского стандарта BS 7799; c) +: международный стандарт ГОСТ Р ИСО/МЭК 27001-2006 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» d) стандарт «Критерии оценки доверенных компьютерных систем» «Оранжевая книга» e) международный стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий»	
215.	d) e)	Какие из перечисленных стандартов относятся к группе оценочных стандартов? (выберите несколько правильных ответов) a) рекомендации X.800, «Архитектура безопасности для взаимодействия открытых систем» – регламентирует методы и средства обеспечения ИБ в компьютерных сетях; b) международный стандарт ISO/IEC 17799 «Практические правила управления информационной безопасностью», разработанный на основе одноименного британского стандарта BS 7799; c) международный стандарт ГОСТ Р ИСО/МЭК 27001-2006 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ». d) +: стандарт «Критерии оценки доверенных компьютерных систем» «Оранжевая книга»	ОПК-5 ОПК-10 ОПК-2.4

		e) +: международный стандарт ISO/IEC 15408 «Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»	
216.	b)	Что содержит ГОСТ Р ИСО/МЭК 15408-1? a) универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам b) +: общий подход к формированию требований и оценке безопасности (функциональные и доверия), основные конструкции (профиль защиты, задание по безопасности) представления требований безопасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ c) систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям	ОПК-5 ОПК-10 ОПК-2.4
217.	a)	Что содержит ГОСТ Р ИСО/МЭК 15408-2? a) +: универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам b) общий подход к формированию требований и оценке безопасности (функциональные и доверия), основные конструкции (профиль защиты, задание по безопасности)	ОПК-5 ОПК-10 ОПК-2.4

		представления требований безопасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ c) систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям	
218.	c)	Что содержит ГОСТ Р ИСО/МЭК 15408-3? a) универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам b) общий подход к формированию требований и оценке безопасности (функциональные и доверия), основные конструкции (профиль защиты, задание по безопасности) представления требований безопасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ c) +: систематизированный каталог требований доверия, определяющих меры, которые должны быть приняты на всех этапах жизненного цикла продукта или системы ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям	ОПК-5 ОПК-10 ОПК-2.4
219.	a)	Для чего предназначены общие критерии в соответствии с ГОСТ Р ИСО/МЭК 15408?	ОПК-5 ОПК-10 ОПК-2.4

		a) +: для использования в качестве основы при оценке характеристик безопасности продуктов и систем информационных технологий (ИТ) b) для представления требований безопасности в интересах потребителей c) для оценки эффективности используемых технических (программных и аппаратных) средств защиты информации; d) для оценки эффективности работы специалистов, ответственных за реагирование на инциденты	
220.	b)	Что понимается под аутентификационными данными в соответствии с ГОСТ Р ИСО/МЭК 15408? a) информация, связанная с субъектами, пользователями и/или объектами, которая используется для осуществления политики безопасности объекта оценки b) +: информация, используемая для верификации предъявленного идентификатора пользователя c) механизм проверки правомочности обращений	ОПК-5 ОПК-10 ОПК-2.4
221.	a) c)	Что понимается под моделью политики безопасности объекта оценки в соответствии с ГОСТ Р ИСО/МЭК 15408? a) +: структурированное представление политики безопасности, которая должна быть осуществлена на объекте оценки b) информация, связанная с субъектами, пользователями и/или объектами, которая используется для осуществления политики безопасности объекта оценки c) +: информация, используемая для верификации предъявленного идентификатора пользователя	ОПК-5 ОПК-10 ОПК-2.4

222.	a)	В каком качестве может использоваться часть 1 ГОСТ Р ИСО/МЭК 15408 потребителем? (выберите несколько правильных ответов) a) +: в качестве общих сведений по применению и как руководство по структуре профилей защиты b) в качестве общих сведений и справочного руководства по разработке требований и формулированию спецификаций безопасности для объектов оценки c) в качестве общих сведений по применению и как руководство по структуре профилей защиты и заданий по безопасности	ОПК-5 ОПК-10 ОПК-2.4
223.	b)	В каком качестве может использоваться часть 1 ГОСТ Р ИСО/МЭК 15408 разработчиком? (выберите несколько правильных ответов) a) в качестве общих сведений по применению и как руководство по структуре профилей защиты b) +: в качестве общих сведений и справочного руководства по разработке требований и формулированию спецификаций безопасности для объектов оценки c) в качестве общих сведений по применению и как руководство по структуре профилей защиты и заданий по безопасности	ОПК-5 ОПК-10 ОПК-2.4
224.	c)	В каком качестве может использоваться часть 1 ГОСТ Р ИСО/МЭК 15408 оценщиком? (выберите несколько правильных ответов) a) в качестве общих сведений по применению и как руководство по структуре профилей защиты b) в качестве общих сведений и справочного руководства по разработке требований и формулированию спецификаций безопасности для объектов оценки	ОПК-5 ОПК-10 ОПК-2.4

		c) +: в качестве общих сведений по применению и как руководство по структуре профилей защиты и заданий по безопасности	
225.	a)	В каком качестве может использоваться часть 2 ГОСТ Р ИСО/МЭК 15408 потребителем? (выберите несколько правильных ответов) a) +: в качестве руководства и справочника при формулировании требований к функциям безопасности b) в качестве справочника по интерпретации функциональных требований и формулированию функциональных спецификаций для объектов оценки c) в качестве обязательного изложения критериев оценки, используемых при определении эффективности выполнения объектом оценки заявленных функций безопасности	ОПК-5 ОПК-10 ОПК-2.4
226.	b)	В каком качестве может использоваться часть 2 ГОСТ Р ИСО/МЭК 15408 разработчиком? (выберите несколько правильных ответов) a) в качестве руководства и справочника при формулировании требований к функциям безопасности b) +: в качестве справочника по интерпретации функциональных требований и формулированию функциональных спецификаций для объектов оценки c) в качестве обязательного изложения критериев оценки, используемых при определении эффективности выполнения объектом оценки заявленных функций безопасности	ОПК-5 ОПК-10 ОПК-2.4
227.	c)	В каком качестве может использоваться часть 2 ГОСТ Р ИСО/МЭК 15408 оценщиком? (выберите несколько правильных ответов)	ОПК-5 ОПК-10 ОПК-2.4

		a) в качестве руководства и справочника при формулировании требований к функциям безопасности b) в качестве справочника по интерпретации функциональных требований и формулированию функциональных спецификаций для объектов оценки c) +: в качестве обязательного изложения критериев оценки, используемых при определении эффективности выполнения объектом оценки заявленных функций безопасности	
228.	a)	В каком качестве может использоваться часть 3 ГОСТ Р ИСО/МЭК 15408 потребителем? (выберите несколько правильных ответов) a) +: в качестве руководства по определению требуемого уровня доверия b) в качестве справочника по интерпретации требований доверия и определению подходов к установлению доверия к объектам оценки c) в качестве обязательного изложения критериев оценки, используемых при определении доверия к объектам оценки и оценке профилей защиты и заданий по безопасности	ОПК-5 ОПК-10 ОПК-2.4
229.	b)	В каком качестве может использоваться часть 3 ГОСТ Р ИСО/МЭК 15408 разработчиком? (выберите несколько правильных ответов) a) в качестве руководства по определению требуемого уровня доверия b) +: в качестве справочника по интерпретации требований доверия и определению подходов к установлению доверия к объектам оценки	ОПК-5 ОПК-10 ОПК-2.4

		c) в качестве обязательного изложения критериев оценки, используемых при определении доверия к объектам оценки и оценке профилей защиты и заданий по безопасности	
230.	c)	В каком качестве может использоваться часть 3 ГОСТ Р ИСО/МЭК 15408 оценщиком? (выберите несколько правильных ответов) a) в качестве руководства по определению требуемого уровня доверия b) в качестве справочника по интерпретации требований доверия и определению подходов к установлению доверия к объектам оценки c) +: в качестве обязательного изложения критериев оценки, используемых при определении доверия к объектам оценки и оценке профилей защиты и заданий по безопасности	ОПК-5 ОПК-10 ОПК-2.4
231.	a)	Что содержит профиль защиты в соответствии с ГОСТ Р ИСО/МЭК 15408? a) +: совокупность требований безопасности, взятых из общих критериев или сформулированных в явном виде, в которую следует включить оценочный уровень доверия (возможно усиленный дополнительными компонентами доверия) b) совокупность требований безопасности, которые могут быть определены ссылками на ПЗ, непосредственно на функциональные компоненты или компоненты доверия из ОК или же сформулированы в явном виде c) базовый набор требований доверия для оценки	ОПК-5 ОПК-10 ОПК-2.4

232.	b)	Что содержит задание по безопасности в соответствии с ГОСТ Р ИСО/МЭК 15408? a) совокупность требований безопасности, взятых из общих критериев или сформулированных в явном виде, в которую следует включить оценочный уровень доверия (возможно усиленный дополнительными компонентами доверия) b) +: совокупность требований безопасности, которые могут быть определены ссылками на профиль защиты, непосредственно на функциональные компоненты или компоненты доверия из общих критериев или же сформулированы в явном виде c) базовый набор требований доверия для оценки	ОПК-5 ОПК-10 ОПК-2.4
233.	c)	Что содержит оценочный уровень доверия в соответствии с ГОСТ Р ИСО/МЭК 15408? a) совокупность требований безопасности, взятых из общих критериев или сформулированных в явном виде, в которую следует включить оценочный уровень доверия (возможно усиленный дополнительными компонентами доверия) b) совокупность требований безопасности, которые могут быть определены ссылками на профиль защиты, непосредственно на функциональные компоненты или компоненты доверия из общих критериев или же сформулированы в явном виде c) +: базовый набор требований доверия для оценки	ОПК-5 ОПК-10 ОПК-2.4
234.	a)	Что понимается под обеспечением доступа к информации только для авторизованных пользователей, имеющих право на доступ к ней (в соответствии с ГОСТ Р ИСО/МЭК 17799-2005)? a) +: конфиденциальность	ОПК-5 ОПК-10 ОПК-2.4

		b) целостность c) доступность	
235.	b)	Что понимается под защитой точности и полноты информации и методов ее обработки (в соответствии с ГОСТ Р ИСО/МЭК 17799-2005)? a) конфиденциальность b) +: целостность c) доступность	ОПК-5 ОПК-10 ОПК-2.4
236.	c)	Что понимается под обеспечением доступности информации и связанных с ней ресурсов авторизованным пользователям при необходимости (в соответствии с ГОСТ Р ИСО/МЭК 17799-2005)? a) конфиденциальность b) целостность c) +: доступность	ОПК-5 ОПК-10 ОПК-2.4
237.	a)	Что включается в договор о приеме на работу (в соответствии с ГОСТ Р ИСО/МЭК 17799-2005)? a) +: сведения об ответственности сотрудника в области информационной безопасности b) уведомления о том, что обрабатываемая информация является конфиденциальной или секретной c) сведения об общих обязанностях по реализации и поддержке политики безопасности, а также о конкретных обязанностях по защите отдельных ресурсов и по выполнению конкретных операций, связанных с безопасностью	ОПК-5 ОПК-10 ОПК-2.4

238.	b)	Что включается в соглашение о конфиденциальности при приеме на работу (в соответствии с ГОСТ Р ИСО/МЭК 17799-2005)? a) сведения об ответственности сотрудника в области информационной безопасности b) +: уведомления о том, что обрабатываемая информация является конфиденциальной или секретной c) сведения об общих обязанностях по реализации и поддержке политики безопасности, а также о конкретных обязанностях по защите отдельных ресурсов и по выполнению конкретных операций, связанных с безопасностью	ОПК-5 ОПК-10 ОПК-2.4
239.	c)	Что включается в права и обязанности в отношении информационной безопасности при приеме на работу (в соответствии с ГОСТ Р ИСО/МЭК 17799-2005)? a) сведения об ответственности сотрудника в области информационной безопасности b) уведомления о том, что обрабатываемая информация является конфиденциальной или секретной c) +: сведения об общих обязанностях по реализации и поддержке политики безопасности, а также о конкретных обязанностях по защите отдельных ресурсов и по выполнению конкретных операций, связанных с безопасностью	ОПК-5 ОПК-10 ОПК-2.4
240.	a)	Что понимается под разделением областей разработки и эксплуатации информационной системы (в соответствии с ГОСТ Р ИСО/МЭК 17799-2005)? a) +: отделение друг от друга области разработки, тестирования и эксплуатации информационной системы	ОПК-5 ОПК-10 ОПК-2.4

		b) метод, позволяющий уменьшить риск случайного или намеренного неправомерного использования информационной системы c) прогноз мощности системы, которая потребуется в будущем, чтобы уменьшить риск перегрузки системы	
241.	b)	Что понимается под разделением полномочий пользователей информационной системы (в соответствии с ГОСТ Р ИСО/МЭК 17799-2005)? a) отделение друг от друга области разработки, тестирования и эксплуатации информационной системы b) +: метод, позволяющий уменьшить риск случайного или намеренного неправомерного использования информационной системы c) прогноз мощности системы, которая потребуется в будущем, чтобы уменьшить риск перегрузки системы	ОПК-5 ОПК-10 ОПК-2.4
242.	c)	Что понимается под планированием разработки и приемки системы обработки информации (в соответствии с ГОСТ Р ИСО/МЭК 17799-2005)? a) отделение друг от друга области разработки, тестирования и эксплуатации информационной системы b) метод, позволяющий уменьшить риск случайного или намеренного неправомерного использования информационной системы c) +: прогноз мощности системы, которая потребуется в будущем, чтобы уменьшить риск перегрузки системы	ОПК-5 ОПК-10 ОПК-2.4

243.	a)	Что понимается под регистрацией пользователей информационной системы (в соответствии с ГОСТ Р ИСО/МЭК 17799-2005)? a) +: официальная процедура регистрации и удаления регистрационных данных пользователей, которая будет использоваться для предоставления доступа ко всем многопользовательским информационным системам и сервисам b) ограничение и контроль распределения и использования привилегий (функций или средств многопользовательской информационной системы, позволяющих определенному пользователю обходить реализованные в системе или приложениях средства защиты) c) контроль предоставления паролей посредством официальной процедуры	ОПК-5 ОПК-10 ОПК-2.4
244.	b)	Что понимается под управлением привилегиями пользователей (в соответствии с ГОСТ Р ИСО/МЭК 17799-2005)? a) официальная процедура регистрации и удаления регистрационных данных пользователей, которая будет использоваться для предоставления доступа ко всем многопользовательским информационным системам и сервисам b) +: ограничение и контроль распределения и использования привилегий (функций или средств многопользовательской информационной системы, позволяющих определенному пользователю обходить реализованные в системе или приложениях средства защиты) c) контроль предоставления паролей посредством официальной процедуры	ОПК-5 ОПК-10 ОПК-2.4

245.	c)	Что понимается под управлением паролями пользователей (в соответствии с ГОСТ Р ИСО/МЭК 17799-2005)? a) официальная процедура регистрации и удаления регистрационных данных пользователей, которая будет использоваться для предоставления доступа ко всем многопользовательским информационным системам и сервисам b) ограничение и контроль распределения и использования привилегий (функций или средств многопользовательской информационной системы, позволяющих определенному пользователю обходить реализованные в системе или приложениях средства защиты) c) +: контроль предоставления паролей посредством официальной процедуры	ОПК-5 ОПК-10 ОПК-2.4
246.	a)	Что понимается под ведением журнала событий (в соответствии с ГОСТ Р ИСО/МЭК 17799-2005)? a) +: ведение контрольных журналов, в которых будут заноситься исключительные ситуации и другие события, связанные с безопасностью b) определение отклонения от политики управления доступом и регистрация событий, которые можно отследить, чтобы иметь улики в случае инцидентов, связанных с безопасностью c) осуществление логического доступа к программному обеспечению и информации только авторизованным пользователям	ОПК-5 ОПК-10 ОПК-2.4

247.	b)	Что понимается под мониторингом доступа и использованием системы (в соответствии с ГОСТ Р ИСО/МЭК 17799-2005)? a) ведение контрольных журналов, в которых будут заноситься исключительные ситуации и другие события, связанные с безопасностью b) +: определение отклонения от политики управления доступом и регистрация событий, которые можно отследить, чтобы иметь улики в случае инцидентов, связанных с безопасностью c) осуществление логического доступа к программному обеспечению и информации только авторизованным пользователям	ОПК-5 ОПК-10 ОПК-2.4
248.	c)	Что понимается под контролем доступа к приложениям (в соответствии с ГОСТ Р ИСО/МЭК 17799-2005)? a) ведение контрольных журналов, в которых будут заноситься исключительные ситуации и другие события, связанные с безопасностью b) определение отклонения от политики управления доступом и регистрация событий, которые можно отследить, чтобы иметь улики в случае инцидентов, связанных с безопасностью c) +: осуществление логического доступа к программному обеспечению и информации только авторизованным пользователям	ОПК-5 ОПК-10 ОПК-2.4
249.	a)	Что понимается под планированием (разработкой) системы менеджмента информационной безопасности (СМИБ) (в соответствии с ГОСТ Р ИСО/МЭК 27001-2006)?	ОПК-5 ОПК-10 ОПК-2.4

		a) +: разработка политики, установление целей, процессов и процедур системы менеджмента информационной безопасности (СМИБ), относящихся к менеджменту риска и улучшению информационной безопасности, для достижения результатов, соответствующих общей политике и целям организации b) внедрение и применение политики информационной безопасности, мер управления, процессов и процедур СМИБ c) оценка, в том числе, по возможности, количественная, результативности процессов относительно требований политики, целей безопасности и практического опыта функционирования СМИБ и информирование высшего руководства о результатах для последующего анализа d) проведение корректирующих и превентивных действий, основанных на результатах внутреннего аудита или другой соответствующей информации, и анализа со стороны руководства в целях достижения непрерывного улучшения СМИБ	
250.	b)	Что понимается под осуществлением (внедрением и обеспечением функционирования) системы менеджмента информационной безопасности (СМИБ) (в соответствии с ГОСТ Р ИСО/МЭК 27001-2006)? a) разработка политики, установление целей, процессов и процедур системы менеджмента информационной безопасности (СМИБ), относящихся к менеджменту риска и улучшению информационной безопасности, для достижения результатов, соответствующих общей политике и целям организации	ОПК-5 ОПК-10 ОПК-2.4

		b) +: внедрение и применение политики информационной безопасности, мер управления, процессов и процедур СМИБ c) оценка, в том числе, по возможности, количественная, результативности процессов относительно требований политики, целей безопасности и практического опыта функционирования СМИБ и информирование высшего руководства о результатах для последующего анализа d) проведение корректирующих и превентивных действий, основанных на результатах внутреннего аудита или другой соответствующей информации, и анализа со стороны руководства в целях достижения непрерывного улучшения СМИБ	
251.	c)	Что понимается под проверкой (проведением мониторинга и анализа) системы менеджмента информационной безопасности (СМИБ) (в соответствии с ГОСТ Р ИСО/МЭК 27001-2006)? a) разработка политики, установление целей, процессов и процедур системы менеджмента информационной безопасности (СМИБ), относящихся к менеджменту риска и улучшению информационной безопасности, для достижения результатов, соответствующих общей политике и целям организации b) внедрение и применение политики информационной безопасности, мер управления, процессов и процедур СМИБ c) +: оценка, в том числе, по возможности, количественная, результативности процессов относительно требований политики, целей безопасности и практического опыта функционирования СМИБ и информирование высшего руководства о результатах для последующего анализа	ОПК-5 ОПК-10 ОПК-2.4

		d) проведение корректирующих и превентивных действий, основанных на результатах внутреннего аудита или другой соответствующей информации, и анализа со стороны руководства в целях достижения непрерывного улучшения СМИБ	
252.	d)	Что понимается под действием (поддержкой и улучшением) системы менеджмента информационной безопасности (СМИБ) (в соответствии с ГОСТ Р ИСО/МЭК 27001-2006)? a) разработка политики, установление целей, процессов и процедур системы менеджмента информационной безопасности (СМИБ), относящихся к менеджменту риска и улучшению информационной безопасности, для достижения результатов, соответствующих общей политике и целям организации b) внедрение и применение политики информационной безопасности, мер управления, процессов и процедур СМИБ c) оценка, в том числе, по возможности, количественная, результативности процессов относительно требований политики, целей безопасности и практического опыта функционирования СМИБ и информирование высшего руководства о результатах для последующего анализа d) +: проведение корректирующих и превентивных действий, основанных на результатах внутреннего аудита или другой соответствующей информации, и анализа со стороны руководства в целях достижения непрерывного улучшения СМИБ	ОПК-5 ОПК-10 ОПК-2.4

253.	b)	К какой стадии аудита информационной безопасности предприятия относится процедура анализа имеющейся политики информационной безопасности предприятия и другой организационной документации? a) инициирование проведения аудита b) +: непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	ОПК-5 ОПК-10 ОПК-2.4
254.	a)	К какой стадии аудита информационной безопасности предприятия относится процедура определения основных угроз, средства защиты от которых необходимо подвергнуть аудиту? a) +: инициирование проведения аудита b) непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	ОПК-5 ОПК-10 ОПК-2.4
255.	a)	К какой стадии аудита информационной безопасности предприятия относится процедура определения перечня обследуемых информационных ресурсов и информационных систем (подсистем)? a) +: инициирование проведения аудита b) непосредственно осуществление сбора информации и проведение обследования аудиторами c) анализ собранных данных и выработка рекомендаций d) подготовка аудиторского отчета и аттестационного заключения	ОПК-5 ОПК-10 ОПК-2.4

2. Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации. Рейтинговая система оценки знаний студентов основана на использовании совокупности контрольных мероприятий по проверке пройденного материала (контрольных точек), оптимально расположенных на всем временном интервале изучения дисциплины. Принципы рейтинговой системы оценки знаний студентов основываются на требованиях, описанных в Положении об организации образовательного процесса на основе рейтинговой системы оценки знаний студентов в ФГАОУ ВО «СКФУ».

Рейтинговая система оценки не предусмотрено для студентов, обучающихся на образовательных программах уровня высшего образования магистратуры, для обучающихся на образовательных программах уровня высшего образования бакалавриата заочной и очно-заочной формы обучения.

3. Критерии оценивания компетенций*

Оценка «отлично» выставляется студенту, если_____
_____

Оценка «хорошо» выставляется студенту, если_____
_____

Оценка «удовлетворительно» выставляется студенту, если_____
_____

Оценка «неудовлетворительно» выставляется студенту, если_____
_____

*Оценка «зачтено» выставляется студенту, если*_____
_____

*Оценка «не зачтено» выставляется студенту, если*_____
_____

**** в соответствии с результатами освоения дисциплины и видами заданий***