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

Комплексная система защиты информации на предприятии
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	7,8

Введение

1. Назначение. Фонд оценочных средств (ФОС) предназначен для текущего контроля успеваемости и промежуточной аттестации по дисциплине «Комплексная система защиты информации на предприятии» 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) «Комплексная система защиты информации на предприятии» 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) Рачков В.Е., доцент 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 «Комплексная система защиты информации на предприятии».

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	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
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 Использует методологический базис теории защиты информации, используемый при разработке формировании политики информационной безопасности*	не оперирует понятиями методологического базиса теории защиты информации и слабо формирует компоненты политики информационной безопасности	в целом оперирует понятиями методологического базиса теории защиты информации и в основном формирует компоненты политики информационной безопасности	в целом оперирует понятиями методологического базиса теории защиты информации и формирует все компоненты политики информационной безопасности	оперирует понятиями методологического базиса теории защиты информации и формирует все компоненты политики информационной безопасности
Результаты обучения по дисциплине (модулю): *Индикатор: ИД-2 Осуществляет организацию и поддерживает выполнение комплекса мер по обеспечению информационной безопасности на объекте защиты в качестве технического специалиста*	не организовывает и не поддерживает выполнение комплекса минимально-допустимых мер по обеспечению информационной безопасности, не управляет процессом их реализации на объекте защиты	организовывает и поддерживает выполнение комплекса минимально-допустимых мер по обеспечению информационной безопасности, управляет процессом их реализации на объекте защиты	организовывает и поддерживает выполнение комплекса основных мер по обеспечению информационной безопасности, управляет процессом их реализации на объекте защиты	организовывает и поддерживает выполнение комплекса исчерпывающих мер по обеспечению информационной безопасности, управляет процессом их реализации на объекте защиты
Результаты обучения по дисциплине (модулю): *Индикатор: ИД-3 Управляет процессом выполнения комплекса мер по обеспечению информационной безопасности реализации на объекте защиты в*	не планирует и не организует управление процессом выполнения комплекса мер по обеспечению информационной безопасности реализации на объекте защиты в качестве технического специалиста	планирует но слабо организует управление процессом выполнения комплекса мер по обеспечению информационной безопасности реализации на объекте защиты в качестве технического специалиста	планирует и в целом организует управление процессом выполнения комплекса мер по обеспечению информационной безопасности реализации на объекте защиты в	планирует и организует управление процессом выполнения комплекса мер по обеспечению информационной безопасности реализации на объекте защиты в качестве

качестве технического специалиста			качестве технического специалиста	технического специалиста
Компетенция: ОПК-2.2 Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы				
Результаты обучения по дисциплине (модулю): *Индикатор:* *ИД-1* *Демонстрирует понимание оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих, а также устойчивости к деструктивным воздействиям на информационные ресурсы предприятия*	- слабо выявляет составляющие процесса оптимизации структуры и функциональных процессов объекта защиты - не формулирует информационные составляющие процесса оптимизации структуры; - не оценивает устойчивость к деструктивным воздействиям на информационные ресурсы предприятия	- в основном выявляет составляющие процесса оптимизации структуры и функциональных процессов объекта защиты - фрагментарно формулирует информационные составляющие процесса оптимизации структуры; - с трудом оценивает устойчивость к деструктивным воздействиям на информационные ресурсы предприятия	- в целом выявляет составляющие процесса оптимизации структуры и функциональных процессов объекта защиты - фрагментарно формулирует информационные составляющие процесса оптимизации структуры; - оценивает устойчивость к деструктивным воздействиям на информационные ресурсы предприятия	- выявляет составляющие процесса оптимизации структуры и функциональных процессов объекта защиты - формулирует информационные составляющие процесса оптимизации структуры; - оценивает устойчивость к деструктивным воздействиям на информационные ресурсы предприятия
Результаты обучения по дисциплине (модулю): Индикатор: *ИД-2* *Демонстрирует способность формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих*	-слабо разрабатывает предложения по оптимизации структуры и функциональных процессов объекта защиты и не берет во внимание его информационные составляющие	-в целом разрабатывает предложения по оптимизации структуры и функциональных процессов объекта защиты, но при этом упускает его информационные составляющие	-в целом разрабатывает предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих	- грамотно и системно разрабатывает предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих
Компетенция: ОПК-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности				

Результаты обучения по дисциплине (модулю): *Индикатор:* *ИД-3* *Демонстрирует знания комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности*	- слабо понимает комплекс мер по обеспечению безопасности объекта защиты; - не формулирует комплекс мер по обеспечению безопасности объекта защиты; - слабо оперирует локальными нормативных актами и стандартами информационной безопасности.	- в основном понимает комплекс мер по обеспечению безопасности объекта защиты; - частично формулирует комплекс мер по обеспечению безопасности объекта защиты; - фрагментарно оперирует локальными нормативных актами и стандартами информационной безопасности.	- в целом понимает комплекс мер по обеспечению безопасности объекта защиты; - частично формулирует комплекс мер по обеспечению безопасности объекта защиты; - оперирует локальными нормативных актами и стандартами информационной безопасности.	- понимает комплекс мер по обеспечению безопасности объекта защиты; - формулирует комплекс мер по обеспечению безопасности объекта защиты; - оперирует локальными нормативных актами и стандартами информационной безопасности.
Результаты обучения по дисциплине (модулю): *Индикатор:* *ИД-4 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности*	- в основном осуществляет разработку комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности; - не планирует внедрение комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности; - слабо реализует сопровождение комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	- в основном осуществляет разработку комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности; - частично планирует внедрение комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности; - фрагментарно реализует сопровождение комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной	- в целом осуществляет разработку комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности; - планирует внедрение комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности; - фрагментарно	- осуществляет разработку комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности; - планирует внедрение комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности; - реализует

		безопасности	реализует сопровождение комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	сопровождение комплекса мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности
Компетенция: ОПК-2.4. Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами				
Результаты обучения по дисциплине (модулю): *Индикатор:* *ИД-3* *Демонстрирует знания процедур аудита защищенности объекта информатизации и нормативных документов, определяющих его содержание*	- слабо оперирует понятиями процедур аудита защищенности объекта информатизации и нормативных документов, определяющих его содержание; - фрагментарно формулирует процедуры аудита защищенности объекта информатизации и нормативные документы, определяющие его содержание; - не понимает сущность процедур аудита защищенности объекта информатизации.	- в основном оперирует понятиями процедур аудита защищенности объекта информатизации и нормативных документов, определяющих его содержание; - фрагментарно формулирует процедуры аудита защищенности объекта информатизации и нормативные документы, определяющие его содержание; - частично понимает сущность процедур аудита защищенности объекта информатизации.	- в целом оперирует понятиями процедур аудита защищенности объекта информатизации и нормативных документов, определяющих его содержание; - фрагментарно формулирует процедуры аудита защищенности объекта информатизации и нормативные документы, определяющие его содержание; - понимает сущность процедур аудита защищенности объекта информатизации.	- оперирует понятиями процедур аудита защищенности объекта информатизации и нормативных документов, определяющих его содержание; - формулирует процедуры аудита защищенности объекта информатизации и нормативные документы, определяющие его содержание; - понимает сущность процедур аудита защищенности объекта информатизации.
Результаты обучения по дисциплине (модулю): *Индикатор:* *ИД-4* *Осуществляет аудит защищенности объекта*	- не планирует аудит защищенности объекта информатизации в соответствии с нормативными документами; - частично устанавливает последовательность мероприятий аудита защищенности объекта	- в основном планирует аудит защищенности объекта информатизации в соответствии с нормативными документами; - фрагментарно устанавливает	- в целом планирует аудит защищенности объекта информатизации в соответствии с нормативными	- планирует аудит защищенности объекта информатизации в соответствии с нормативными

информатизации в соответствии с нормативными документами	информатизации в соответствии с нормативными документами; - слабо участвует в процедуре аудита защищенности объекта информатизации в соответствии с нормативными документами	последовательность мероприятий аудита защищенности объекта информатизации в соответствии с нормативными документами; - частично участвует в процедуре аудита защищенности объекта информатизации в соответствии с нормативными документами.	документами; - частично устанавливает последовательность мероприятий аудита защищенности объекта информатизации в соответствии с нормативными документами; - участвует в процедуре аудита защищенности объекта информатизации в соответствии с нормативными документами.	документами; - устанавливает последовательность мероприятий аудита защищенности объекта информатизации в соответствии с нормативными документами; - участвует в процедуре аудита защищенности объекта информатизации в соответствии с нормативными 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 7, 8	
1.		Понятие и сущность КСЗИ	ОПК-10
2.		Перечислите методологические основы организации КСЗИ	ОПК-10
3.		Методика определения состава защищаемой информации	ОПК-10
4.		Значение носителей защищаемой информации как объектов защиты	ОПК-10
5.		Как происходит определение источников дестабилизирующего воздействия на информацию ивидов их воздействия?	ОПК-10

6.		В чем заключается методика выявления каналов несанкционированного доступа кинформации?	ОПК-10
7.		Обеспечение полноты составляющих защиты	ОПК-10
8.		Понятие модели объекта, основные виды моделей и их характеристика	ОПК-10
9.		Модель как инструмент количественного и качественного анализа комплексной системызащиты информации	ОПК-2.2
10.		Общее содержание работ по организации комплексной системы защиты информации	ОПК-2.2
11.		В чем заключается организационное построение комплексной системы защиты информации?	ОПК-2.2
12.		Как происходит определение состава кадрового обеспечения функционирования комплекснойсистемы защиты информации?	ОПК-2.2
13.		Значение материально-технического обеспечения функционирования комплексной системызащиты информации	ОПК-2.2

14.		Понятие нормативно-методического обеспечения комплексной системы защиты информации	ОПК-2.2
15.		Понятие и цели управления комплексной системы защиты информации	ОПК-2.2
16.		Назовите особенности функций управления комплексной системой защиты информации	ОПК-2.2
17.		Понятие и задачи планирования функционирования комплексной системы защитыинформации	ОПК-2.3
18.		Понятие и виды контроля функционирования комплексной системы защиты информации	ОПК-2.3
19.		Понятие и основные виды чрезвычайных ситуаций	ОПК-2.3
20.		Приведите классификацию подходов к оценке эффективности систем защиты информации	ОПК-2.3
21.		Приведите классификационную структуру методов и моделей оценки	ОПК-2.3
22.		В чём состоит назначение КСЗИ?	ОПК-2.3
23.		КСЗИ как сложная человеко-машинная система	ОПК-2.3
24.		Охарактеризуйте этапы работы по выявлению состава защищаемой информации.	ОПК-2.3
25.		В чем заключается методика выявления состава носителей защищаемой информации?	ОПК-2.4
26.		В чем заключается методика выявления способов воздействия на информацию?	ОПК-2.4
27.		Определение возможных методов несанкционированного доступа к защищаемой информации	ОПК-2.4
28.		Перечислите факторы и обстоятельства, оказывающих влияние на качество защиты	ОПК-2.4
29.		Значение моделирования процессов комплексной системы защиты информации	ОПК-2.4

		Дайте характеристику основных стадий создания комплексной системы защиты информации	
30.		Технологическое построение комплексной системы защиты информации	ОПК-2.4
31.		Распределение функций по защите информации между руководством предприятия, службой защиты информации, специальными комиссиями и пользователями защищаемой информации, обеспечение взаимодействия между ними.	ОПК-2.4
32.		.Как происходит определение состава материально-технического обеспечения? От чего онзависит?	ОПК-2.4
33.		Охарактеризуйте структуру нормативно-методического обеспечения комплексной системызащиты информации	ОПК-2.4
34.		В чем сущность процессов управления комплексной системы защиты информации?	ОПК-2.4
35.		Содержание функций управления комплексной системой защиты информации	ОПК-2.4
36.		Перечислите и охарактеризуйте способы и стадии планирования	ОПК-2.4
37.		Какова цель проведения контрольных мероприятий в комплексной системе защитыинформации?	ОПК-2.4
38.		Перечислите факторы, влияющие на принятие решений в условиях чрезвычайной ситуации	ОПК-2.4
39.		Вероятностный подход: структуризация предметной области оценки, анализ вероятностиреализации угроз безопасности, расчетные соотношения	ОПК-2.4
40.		1. Перечислите базовые понятия и определения, используемые в моделях.	ОПК-2.4
41.	верно	Укажите верно или неверно представленное положение: КСЗИ предприятия есть совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации	ОПК-2.4

42.	верно	Укажите верно или неверно представленное положение: Главной целью КСЗИ является обеспечение непрерывности, устойчивого функционирования предприятия и предотвращения угроз его безопасности.	ОПК-2.4
43.	a b c	Выберите один или несколько ответов: Комплексная система защиты информации направлена: a) на защиту законных интересов организации от противоправных посягательств b) недопущение уничтожения имущества и ценностей c) недопущение разглашения, утечки и несанкционированного доступа к служебной информации d) изоляции работы технических средств обеспечения производственной деятельности, включая информационные технологии	ОПК-2.4
44.	a b c d	Выберите один или несколько ответов: К задачам КСЗИ, можно отнести: a) прогнозирование, своевременное выявление и устранение угроз безопасности персоналу и ресурсам предприятия, причин и условий, способствующих нанесению финансового, материального и морального ущерба, нарушению его нормального функционирования и развития b) эффективное пресечение угроз персоналу и посягательств на ресурсы на основе правовых, организационных и инженерно-технических мер и средств обеспечения безопасности c) отнесение информации к категории ограниченного доступа (служебной и коммерческой тайнам, иной конфиденциальной информации, подлежащей защите от неправомерного использования), а других ресурсов — к различным уровням уязвимости (опасности), подлежащих сохранению d) создание механизма и условий оперативного реагирования на угрозы безопасности проявления негативных тенденций в функционировании предприятия e) создание условий для исключения возмещения и локализации наносимого ущерба неправомерными действиями	ОПК-2.4

45.	a b c d	Выберите один или несколько ответов: Обеспечение безопасности предприятия должно основываться на следующих основных принципах: a) Принцип своевременности b) Принцип комплексности c) Принцип непрерывности d) Принцип системности e) Принцип сложности применения	ОПК-2.4
46.	a b c d	Выберите один или несколько ответов: Информация — это: a) сведения о явлениях и процессах независимо от формы их представления b) сведения о лицах c) упорядоченный набор структурированной информации d) сведения о предметах e) сведения о фактах и событиях	ОПК-2.4
47.	a b c	Выберите один или несколько ответов: С точки зрения потребителя качество используемой информации позволяет: a) получать дополнительный моральный эффект b) получать дополнительный физический эффект c) получать дополнительный информационный эффект d) получать дополнительный экономический эффект	ОПК-2.4
48.	a b c d	Выберите один или несколько ответов: Анализ состояния дел в сфере защиты информации показывает, что уже сложилась вполне сформировавшаяся концепция и структура защиты, основу которой составляют: a) наличие значительного практического опыта и наработок b) весьма развитый арсенал технических средств защиты информации, производимых на промышленной основе c) не достаточно четко очерченная система взглядов на эту проблему d) значительное число фирм, специализирующихся на решении	ОПК-2.4

		вопросов защиты информации	
49.	a b c	Выберите один или несколько ответов: Защита информации – это: a) деятельность, направленная на предотвращение утечки защищаемой информации b) деятельность, направленная на организационное и техническое сопровождение информационных процессов в организации c) деятельность, направленная на предотвращение несанкционированных воздействий на защищаемую информацию d) деятельность, направленная на предотвращение непреднамеренных воздействий на защищаемую информацию	ОПК-2.4
50.	a b c d	Выберите один или несколько ответов: Организация и функционирование комплексной системы безопасности должны осуществляться на основе следующих принципов: a) Оперативность b) Своевременность c) Комплексность d) Непрерывность e) Активность	ОПК-2.4
51.	Неверно	Выберите один ответ: Обеспечение безопасности информации - это фрагментарный процесс, заключающийся в обосновании и реализации наиболее рациональных форм, методов, способов и путей создания, совершенствования и развития системы безопасности, непрерывном управлении ею, контроле, выявлении ее узких мест и потенциальных угроз фирме.	ОПК-2.4
52.	Неверно	Выберите один ответ: Информационная безопасность может быть обеспечена лишь при избирательном	ОПК-2.4

		использовании арсенала средств защиты и противодействия во всех структурных элементах производственной системы	
53.	Неверно	Выберите один ответ: Наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый целостный механизм	ОПК-2.4
54.	Верно	Выберите один ответ: Никакая фирма не может обеспечить требуемый уровень безопасности без надлежащий подготовки персонала и пользователей, соблюдения ими всех установленных правил, направленных на обеспечение информационной безопасности.	ОПК-2.4
55.	a b c	Выберите один или несколько ответов: Организация и функционирование комплексной системы защиты информации осуществляется на основе принципа комплексности, сущность которого состоит: a) в упреждающем характере мер обеспечения информационной безопасности b) в обеспечении безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их обработки (преобразования) и использования, во всех режимах функционирования c) в способности системы к развитию и совершенствованию в соответствии с изменениями условий функционирования фирмы d) в обеспечении безопасности персонала, материальных и финансовых ресурсов от возможных угроз всеми доступными законными средствами, методами и мероприятиями	ОПК-2.4
56.	b c d	Выберите один или несколько ответов: Своевременность предполагает постановку задач: a) на основе анализа обстановки b) на стадиях разработки системы безопасности в режиме реального времени c) на основе разработки эффективных мер предупреждения посягательств на законные интересы d) на основе прогнозирования обстановки	ОПК-2.4
57.	c	Выберите один или несколько ответов:	ОПК-2.4

	d	Комплексная система защиты информации на предприятии – это: a) совокупность мероприятий, осуществляемых в целях защиты предприятия от реальных или потенциальных действий физических или юридических лиц, которые могут привести к существенным потерям b) совокупность мероприятий исключительно правового характера c) совокупность взаимосвязанных мероприятий организационно-правового характера d) совокупность мероприятий исключительно технического характера	
58.	a b c	Выберите один или несколько ответов: Целями комплексной системы защиты информации являются: a) Создание условий для коренного изменения технологического процесса на предприятии b) Повышение имиджа и роста прибылей за счет обеспечения качества услуг и безопасности клиентов c) Защита прав предприятия, его структурных подразделений и сотрудников d) Сохранение и эффективное использование финансовых, материальных и информационных ресурсов	ОПК-2.4
59.	a b d	Выберите один или несколько ответов: Задачами комплексной системы защиты информации являются: a) Своевременное выявление и устранение угроз персоналу и ресурсам; причин и условий, способствующих нанесению финансового, материального и морального ущерба интересам фирмы, нарушению ее нормального функционирования и развития b) Создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании фирмы c) Исключение пресечения посягательств на ресурсы и угроз персоналу на основе комплексного подхода к безопасности d) Отнесение информации к категории ограниченного доступа (служебной и коммерческой тайнам, иной конфиденциальной информации, подлежащей защите от неправомерного использования) и других ресурсов — к различным уровням уязвимости (опасности) и подлежащих сохранению	ОПК-2.4

60.	a b c	Выберите один или несколько ответов: К требованиям, предъявляемым к комплексной системе защиты информации можно отнести: a) Четкость определения полномочий и прав пользователей на доступ к определенным видам информации b) Сведения к минимуму числа общих для нескольких пользователей средств защиты c) Учет случаев и попыток НСД к конфиденциальной информации d) Исключение предоставления пользователям минимальных полномочий, необходимых для выполнения порученной работы	ОПК-2.4
61.	Верно	Выберите один ответ: Системы защиты информации относятся к классу сложных систем.	ОПК-2.4
62.	a b c	Выберите один или несколько ответов: Для комплексных систем защиты информации характерны следующие принципы построения: a) Фиксированная архитектура КСЗИ b) Параллельная разработка комплексных систем и систем защиты информации c) Многоуровневая структура построения КСЗИ d) Системный подход к построению КСЗИ	ОПК-2.4
63.	a b c	Выберите один или несколько ответов: Комплексность защиты информации позволяет использовать в оптимальном сочетании: a) Технических методов и средств защиты b) Программных методов и средств защиты c) Нормативных методов защиты d) Криптографических методов и средств защиты	ОПК-2.4
64.	Неверно	Выберите один ответ: Комплексные системы защиты информации не должны иметь централизованное управление	ОПК-2.4
65.	a b	Выберите один или несколько ответов: Основными этапами создания КСЗИ являются:	ОПК-2.4

	c d	a) Рабочее проектирование b) Техническое проектирование c) Организационное проектирование d) Разработка технического задания e) Эскизное проектирование	
66.	e	Выберите один или несколько ответов: Современный опыт решения проблем информационной безопасности показывает, что для достижения наибольшего эффекта при организации защиты информации необходимо руководствоваться рядом принципов. К какому принципу мы можем отнести это содержание: a) принцип комплексности b) принцип прозрачности c) принцип непрерывности d) принцип многоразовости e) нет такого принципа	ОПК-2.4
67.	b	Выберите один или несколько ответов: Современный опыт решения проблем информационной безопасности показывает, что для достижения наибольшего эффекта при организации защиты информации необходимо руководствоваться рядом принципов. К какому принципу мы можем отнести это содержание: использование всего арсенала имеющихся средств защиты во всех структурных элементах производства и на всех этапах технологического цикла обработки информации a) принцип комплексности b) принцип прозрачности c) принцип непрерывности d) принцип многоразовости	ОПК-2.4
68.	a	Выберите один или несколько ответов: Что характеризует это определение: организованная совокупность органов, средств, методов и мероприятий, обеспечивающих защиту информации от разглашения, утечки и несанкционированного доступа к	ОПК-2.4

		ней. a) Информационная система b) Информационная технология c) Система информационной безопасности d) Государственная система обеспечения безопасности	
69.	a b c d	Выберите один или несколько ответов: К важнейшим условиям обеспечения информационной безопасности можно отнести: a) ответственность персонала и руководства b) соблюдение баланса интересов личности и предприятия c) достаточность d) законность e) высокий профессионализм представителей службы информационной безопасности	ОПК-2.4
70.	c	Выберите один или несколько ответов: С позиций системного подхода для реализации принципов обеспечения информационной безопасности процесс, да и сама система защиты информации должны отвечать некоторой совокупности требований, а именно: a) активной b) конкретной и целенаправленной c) стандартной d) централизованной e) плановой	ОПК-2.4
71.			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, если студент показал глубокое, прочное и аргументированное освоение программного учебного материала, при этом поставленный вопрос раскрыт последовательно, четко и логически стройно, в полном исчерпывающем объеме, основные категории, понятия и термины учебного курса формулировались правильно, не допущено при ответе ошибок

Оценка «хорошо» выставляется, если студент показал твердое знание программного учебного материала, при этом поставленный вопрос раскрыт грамотно и по существу, в достаточно полном объеме, основные категории, понятия и термины учебного курса формулировались правильно, допущены при ответе отдельные неточности или одна ошибка;

Оценка «удовлетворительно» выставляется, если студент показал знание только основной части учебного материала без его частных деталей, при этом поставленный вопрос раскрыт с нарушением логической последовательности, не в полном объеме, были допущены неточные формулировки основных категорий, понятий и терминов учебного курса, а также ошибки (не более двух) или ряд незначительных неточностей, не исказивших существенно суть ответа;

Оценка «неудовлетворительно» выставляется, студенту, который не знает значительной части программного материала, допускает грубые ошибки (более двух), существенно исказившие его суть. Оценка неудовлетворительно выставляется также, если отсутствует письменный ответ на вопрос, либо студент отказался его сдавать.