МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

УТВЕРЖДАЮ
Директор Пятигорского института (филиал) СКФУ
_____ Т.А. Шебзухова
«__» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Основы управления информационной безопасностью

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Направление подготовки/специальность 10.03.01 Информационная безопасность
Квалификация выпускника: бакалавр
Форма обучения очная
Год начала обучения 2021
Изучается в 8 семестре

г. Пятигорск 20__ г.

1. Цель и задачи освоения дисциплины

Целью освоения дисциплины «Основы управления информационной безопасностью» является формирование набора профессиональных компетенций будущего бакалавра по направлению подготовки 10.03.01 «Информационная безопасность».

В соответствии с указанной целью при изучении данной дисциплины ставятся следующие задачи:

- анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов;
- разработка предложений по совершенствованию системы управления информационной безопасностью;
- формирование комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.

2. Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части дисциплин Б1. Ее освоение происходит в 8 семестре.

3. Связь с предшествующими дисциплинами

Пререквизитами являются дисциплины: «Основы управленческой деятельности», «Защита и обработка конфиденциальных документов», «Защита информационных процессов в компьютерных системах», «Организационное и правовое обеспечение информационной безопасности».

4. Связь с последующими дисциплинами

Полученные в ходе изучения данной дисциплины профессиональные и общекультурные компетенции необходимы при сдаче ГИА.

5. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

5.1 Наименование компетенций

Код	Формулировка:
ОК-5	способность понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
ОПК-7	способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты
ПК-3	способность администрировать подсистемы информационной безопасности объекта защиты
ПК-4	способность участвовать в работах по реализации политики информационной безопасности,

	применять комплексный подход к обеспечению информационной безопасности объекта защиты
ПК-5	способность принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
ПК-6	способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации
ПК-13	способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
ПК-14	Способностью организовать работу малого коллектива исполнителей в профессиональной деятельности
ПК-15	Способностью организовать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

5.2 Знания, умения и навыки и (или) опыт деятельности, характеризующие этапы формирования компетенций

Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: ▪ современное состояние проблем хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации в организациях и на предприятиях различных направлений деятельности и различных форм собственности	**ОК-5**
Знать: ▪ угрозы информационной безопасности объектов информатизации; ▪ способы несанкционированного доступа к конфиденциальной информации на объекты информатизации. **Владеть:** ▪ навыками обнаружения вторжений на объекты информатизации.	**ОПК-7**
Знать: ▪ об объектах и методах администрирования; **Уметь:** ▪ инсталлировать ПО информационных систем.	**ПК-3**
Уметь: ▪ оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов.	**ПК-4**
Знать: ▪ регламентирующие документы в области проектирования и эксплуатации современных систем охраны информации.	**ПК-5**
Уметь: ▪ формировать предложения по оптимизации комплекса технических средств, применяемых в процессе защищаемого объекта и его информационных составляющих	**ПК-6**

Уметь: ▪ формировать предложения по оптимизации комплекса технических средств, применяемых в процессе защищаемого объекта и его информационных составляющих	**ПК-13**
Владеть: ▪ навыками организации работы малого коллектива исполнителей в процессе защиты объекта	**ПК-14**
Знать: ▪ технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами	**ПК-15**

6. Объем учебной дисциплины/модуля

	Астр. часы	
Объем занятий: Итого	81ч.	3 з.е.
В том числе аудиторных	36 ч.	
Из них:		
Лекций	18 ч.	
Практических работ	18 ч.	
Самостоятельной работы	18 ч.	
Контроль	27 ч.	
Экзамен	8 семестр	

7. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества астрономических часов и видов занятий

7.1 Тематический план дисциплины

№	Раздел (тема) дисциплины	Реализуемые компетенции	Контактная работа обучающихся с преподавателем, часов				Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	
8 семестр							
1.	Тема 1. Основные положения и терминология. Введение в понятие основы управления информационной безопасностью	ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	1,5	1,5			1,5
2.	Тема 2. Документация по комплексной правовой защите информации на предприятии	ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6,	1,5	1,5			1,5

		ПК-13, ПК-14, ПК-15					
3.	Тема 3. Мотивация к обеспечению информационной безопасности на предприятии.	ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	3	3			3
4.	Тема 4. Процесс управления информационной безопасностью.	ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	1,5	1,5			1,5
5.	Тема 5. Этапы создания системы управления ИБ.	ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	1,5	1,5			1,5
6.	Тема 6. Оценка информационных рисков. Управление рисками. Основные понятия	ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	3	3			3
7.	Тема 7. Протоколирование и аудит. Активный аудит	ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	1,5	1,5			1,5
8.	Тема 8. Современные методы и средства анализа и управление рисками информационных систем компаний	ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	1,5	1,5			1,5
9.	Тема 9. Организационно-правовые формы управления безопасностью	ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	3	3			3
	Итого за 8 семестр		18	18			18
	Итого		18	18			18

7.2 Наименование и содержание лекций

№ темы	Наименование тем дисциплины, их краткое содержание	Объем часов	Интерактивная форма проведения
1.	**Тема:** Основные положения и терминология. Введение в понятие основы управле-ния информационной безопасностью *Основные понятия и определения по теме. Управление. Циклическая модель улучшения процессов Основные определения и критерии классификации угроз*	1,5	
2.	**Тема:** Документация по комплексной правовой	1,5	

	защите информации на предприятии . *- «Оранжевая книга» как оценочный стандарт.* *- Критерии оценки безопасности информационных систем* *- Стандарты управления информационной безопасностью.*		
3.	**Тема:** Мотивация к обеспечению информационной безопасности на предприятии. *- Процесс оценки риска информационной безопасности.* *- Идентификация уязвимостей и построение модели нарушителя.* *- Предварительный анализ информационной безопасности предприятия.*	3	
4.	**Тема:** Процесс управления информационной безопасностью.. *- Существующие и планируемые средства контроля.* *- Программные средства защиты информации на предприятии.* *- Аппаратные средства защиты информации на предприятии.*	1,5	
5.	**Тема:** Этапы создания системы управления ИБ.. − *Принятие решения о создании СУИБ.* − *Подготовка к созданию СУИБ.* − *Анализ рисков.* − *Разработка политик и процедур СУИБ.* − *Внедрение СУИБ в эксплуатацию.*	1,5	
6.	**Тема:** Оценка информационных рисков. Управление рисками. Основные понятия. − *идентификация всех активов в рамках выбранной области деятельности;* − *определение ценности идентифицированных активов;* − *идентификация угроз и уязвимостей для идентифицированных активов;* − *оценка рисков для возможных случаев успешной реализации угроз информационной безопасности в отношении идентифицированных активов;* − *выбор критериев принятия рисков;* *подготовка плана обработки рисков.*	3	
7.	**Тема:** Протоколирование и аудит. Активный аудит. *Характерная особенность протоколирования и аудита. Задача активного аудита. Средства активного аудита.*	1,5	
8.	**Тема:** Современные методы и средства анализа и управление рисками информационных систем компаний. *Актуальность задачи обеспечения информационной безопасности для бизнеса. Обоснование необходимости инвестиций в информационную безопасность компании. Программные комплексы анализа и контроля информационных рисков:*	1,5	

	британский CRAMM (компания Insight Consulting), американский RiskWatch (компания RiskWatch) и российский ГРИФ (компания Digital Security).		
9.	**Тема:** Организационно-правовые формы управления безопасностью. *В целях непосредственного выполнения функций по обеспечению безопасности государством образуются специальные органы обеспечения безопасности.*	3	
	Итого	**18**	

7.3 Наименование лабораторных работ

Лабораторные занятия учебным планом не предусмотрены

7.4 Наименование практических занятий

№ Темы	Наименование тем дисциплины, их краткое содержание	Объем часов	Интерактивная форма проведения
8 семестр			
Тема 1. Основные положения и терминология. Введение в понятие основы управления информационной безопасностью			
1.	**Практическая работа №1 «Основополагающие документы в области информационной безопасности»** *изучить основополагающие документы в области информационной безопасности и российские и международные, которые используются в России*	1,5	
Тема 2. Документация по комплексной правовой защите информации на предприятии			
2.	Практическая работа №2 **Тема: Обеспечение информационной безопасности в ведущих зарубежных странах** *ознакомление с основными принципами обеспечения информационной безопасности в ведущих зарубежных странах*	1,5	
Тема 3. Мотивация к обеспечению информационной безопасности на предприятии.			
3.	Практическая работа № 3 **Тема: «Требования и показатели защищенности автоматизированных средств обработки информации»** *ознакомиться с требованиями и показателями защищенности автоматизированных средств обработки информации*	3	
Тема 4. Процесс управления информационной безопасностью.			
4.	Практическая работа № 4 **Тема: «Алгоритмы поведения вирусных и других вредоносных программ»** *Знакомство с некоторыми алгоритмами поведения вирусных и других вредоносных программ.*	1,5	
Тема 5. Этапы создания системы управления ИБ.			
5.	Практическая работа № 5 ***Тема: «Процедура аутентификации пользователя на основе***	1,5	

	пароля» *изучение технологии аутентификации пользователя на основе пароля.*		
Тема 6. Оценка информационных рисков. Управление рисками. Основные понятия			
6.	Практическая работа № 6 **«Анализ рисков информационной безопасности»** *ознакомиться с алгоритмами оценки риска информационной безопасности*	3	
Тема 7. Протоколирование и аудит. Активный аудит			
7.	Практическая работа № 7 **Тема: «Типовые» каналы утечки информации объектов информатизации ОВД. Условия и факторы, способствующие утечке информации ограниченного доступа. Модели возможных нарушителей»** *ознакомиться с условиями и факторами, способствующими утечке информации ограниченного доступа*	1,5	
Тема 8. Современные методы и средства анализа и управление рисками информационных систем компаний			
8.	Практическая работа №8 **Тема: «Предварительный анализ информационной безопасности предприятия»** *Изучить деятельность определенной организации и провести предварительный анализ ее информационной безопасности*	1,5	
Тема 9. Организационно-правовые формы управления безопасностью			
9.	Практическая работа № 9 **Тема: «Построение концепции информационной безопасности предприятия»** *: знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры*	1,5	
	Итого	**18**	

7.5 Технологическая карта самостоятельной работы обучающегося

Технологическая карта

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-	Изучение литературы по темам 1-9	Конспект	собеседование	69,66	7,74	77,4

15						
ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	проработка лекционного материала	Конспект	▪ собеседование	1,62	0,18	1,8
ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	подготовка к практическим занятиям	индивидуальное задание	▪ отчет письменный	1,62	0,18	1,8
			Итого	72,9	8,1	81

8. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

8.1 Перечень компетенций с указанием этапов их формирования в процессе освоения ОП ВО. Паспорт фонда оценочных средств

Код оцениваемой компетенции	**Этап формирования компетенции (№ темы)**	**Средства и технологии оценки**	**Тип контроля (текущий/ промежуточный)**	**Вид контроля (текущий/промежуточный)**	**Наименование оценочного средства**
ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	1-9	отчёт	текущий	письменный, с помощью технических средств	Темы индивидуальных заданий для практических занятий
ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	1-9	конспект	текущий	устный	Вопросы для собеседования
ОК-5, ОПК-7, ПК-3, ПК-4, ПК-5, ПК-6, ПК-13, ПК-14, ПК-15	1-17	Собесе-дование	промежуточный	устный	Вопросы к экзамену
					Вопросы для проверки уровня знаний
					Вопросы (задания) для проверки умений и навыков

8.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкалы оценивания

Уровни сформированности компетенций	Индикаторы	Дескрипторы			
		2 балла	**3 балла**	**4 балла**	**5 баллов**
(для каждой компетенции)		ОК-5			
Базовый	**Уметь:** ▪ работы по установке, настройке и обслуживанию ТСЗИ; ▪ оценивать эффективность применяемых ТСЗИ; ▪ проводить анализ исходных данных для проектирования подсистемы противодействия утечки информации по техническим каналам утечки на объекте информатизации; ▪ вырабатывать обоснованные проектные решения по обеспечению защиты информации	Не умеет: ▪ работы по установке, настройке и обслуживанию ТСЗИ; ▪ оценивать эффективность применяемых ТСЗИ; ▪ проводить анализ исходных данных для проектирования подсистемы противодействия утечки информации по техническим каналам утечки на объекте информатизации; ▪ вырабатывать обоснованные проектные решения по обеспечению защиты информации	Не достаточно хорошо умеет: ▪ работы по установке, настройке и обслуживанию ТСЗИ; ▪ оценивать эффективность применяемых ТСЗИ; ▪ проводить анализ исходных данных для проектирования подсистемы противодействия утечки информации по техническим каналам утечки на объекте информатизации; ▪ вырабатывать обоснованные проектные решения по обеспечению защиты информации	Умеет: ▪ работы по установке, настройке и обслуживанию ТСЗИ; ▪ оценивать эффективность применяемых ТСЗИ; ▪ проводить анализ исходных данных для проектирования подсистемы противодействия утечки информации по техническим каналам утечки на объекте информатизации; ▪ вырабатывать обоснованные проектные решения по обеспечению защиты информации	
	ОПК-7				
	Знать: ▪ классификацию, характеристики технических каналов утечки	Не знает: ▪ классификацию, характеристики технических	Не достаточно хорошо знает классификацию, характеристики технических	Знает ▪ классификацию, характеристики технических каналов утечки	

	информации, возможности технических разведок; ▪ методы, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.	каналов утечки информации, возможности технических разведок; ▪ методы, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.	каналов утечки информации, возможности технических разведок; ▪ методы, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.	информации, возможности технических разведок; ▪ методы, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации.	
	ПК-3				
	Знать порядок организации и проведения аттестации объектов информатизации на соответствие требованиям по защите информации	Не знает порядок организации и проведения аттестации объектов информатизации на соответствие требованиям по защите информации	Не достаточно знает порядок организации и проведения аттестации объектов информатизации на соответствие требованиям по защите инфомации	Знает на достаточно хорошем уровне порядок организации и проведения аттестации объектов информатизации на соответствие требованиям по защите инфор-мации	
	ПК-4				
	Уметь: ▪ осуществлять технические мероприятия по обеспечению защиты информации от ее утечки по техническим каналам с учетом организационной структуры объекта защиты и вероятных угроз; ▪ проводит	▪ Не умеет осуществлять технические мероприятия по обеспечению защиты информации от ее утечки по техническим каналам с учетом организационной структуры объекта	▪ Не достаточно хорошо осуществляет технические мероприятия по обеспечению защиты информации от ее утечки по техническим каналам с учетом организационной структуры объекта защиты и	▪ Достаточно хорошо умеет осуществлять технические мероприятия по обеспечению защиты информации от ее утечки по техническим каналам с учетом организационной структуры объекта защиты и	

	ь специальные исследования технических средств и систем для аттестации объектов на соответствие требованиям нормативных документов; ▪ выполнять мероприятия по эксплуатации технических средств защиты информации от ее утечки по техническим каналам	защиты и вероятных угроз; ▪ проводить специальные исследования технических средств и систем для аттестации объектов на соответствие требованиям нормативных документов; выполнять мероприятия по эксплуатации технических средств защиты информации от ее утечки по техническим каналам	вероятных угроз; ▪ проводить специальные исследования технических средств и систем для аттестации объектов на соответствие требованиям нормативных документов; ▪ выполнять мероприятия по эксплуатации технических средств защиты информации от ее утечки по техническим каналам	вероятных угроз; ▪ проводить специальные исследования технических средств и систем для аттестации объектов на соответствие требованиям нормативных документов; ▪ выполнять мероприятия по эксплуатации технических средств защиты информации от ее утечки по техническим каналам	
	ПК-5				
	Уметь проводить экспериментальные исследования технических средств и систем с учетом требований по обеспечению информационной безопасности по методикам нормативных документов ФСТЭК.	Не умеет проводить экспериментальные исследования технических средств и систем с учетом требований по обеспечению информационной безопасности по методикам нормативных документов ФСТЭК.	Не достаточно хорошо проводит экспериментальные исследования технических средств и систем с учетом требований по обеспече-нию информационной безопасно-сти по мето-дикам нор-мативных документов	Достаточно хорошо умеет проводить экспериментальные исследования технических средств и систем с учетом требований по обеспечению информационной безопасности по методикам нормативных документов ФСТЭК.	
	ПК-6				
	Уметь: ▪ выявлять сущность проблем, возникающих в ходе профессиональной деятельности	Не умеет: ▪ выявлять сущность проблем, возникающих в ходе профессионал	Не достаточно хорошо: ▪ выявляет сущность проблем, возникающих в ходе профессиональ	Достаточно хорошо умеет: ▪ выявлять сущность проблем, возникающих в ходе профессиональ	

	путем анализа и оценки угроз ИБ для технических средств и систем объекта информатизации; ▪ формировать комплекс мер по обеспечению защиты информации от ее утечки по техническим каналам с учетом их технической реализуемости. **Владеть:** ▪ навыками работы с нормативными правовыми актами и методическими документами в области ТЗИ; навыками безопасного применения ТСЗИ в профессиональной деятельности.	ьной деятельности путем анализа и оценки угроз ИБ для технических средств и систем объекта информатизации; ▪ формировать комплекс мер по обеспечению защиты информации от ее утечки по техническим каналам с учетом их технической реализуемости. **Владеть:** ▪ навыками работы с нормативными правовыми актами и методическими документами в области ТЗИ; ▪ навыками безопасного применения ТСЗИ в профессиональной деятельности	ной деятельности путем анализа и оценки угроз ИБ для технических средств и систем объекта информатизации; ▪ формировать комплекс мер по обеспечению защиты информации от ее утечки по техническим каналам с учетом их технической реализуемости. **Владеть:** ▪ навыками работы с нормативными правовыми актами и методическими документами в области ТЗИ; ▪ навыками безопасного применения ТСЗИ в профессиональной деятельности	ной деятельности путем анализа и оценки угроз ИБ для технических средств и систем объекта информатизации; ▪ формировать комплекс мер по обеспечению защиты информации от ее утечки по техническим каналам с учетом их технической реализуемости. **Владеть:** ▪ навыками работы с нормативными правовыми актами и методическими документами в области ТЗИ; ▪ навыками безопасного применения ТСЗИ в профессиональной деятельности	
	ПК-13				
	Знать организационные и методические проблемы автоматизации делопроизводственных операций по документам	Не знает организационные и методические проблемы автоматизации делопроизводственных операций по	Не достаточно знает хорошо организационные и методические проблемы автоматизации делопроизводственных операций по	Знает на достаточно хорошем уровне организационные и методические проблемы автоматизации делопроизводс	

		документам	документам	твенных операций по документам	
	ПК-14				
	Уметь: определять угрозы безопасности конфиденциальной информации	Не умеет определять угрозы безопасности конфиденциальной информации	Не достаточно хорошо умеет определять угрозы безопасности конфиденциальной информации	Достаточно хорошо умеет определять угрозы безопасности конфиденциальной информации	
	ПК-15				
	Владеет навыками определения угроз безопасности информации и возможные пути противодействия им	Владеет навыками определения угроз безопасности информации, но не применяет возможные пути противодействия им	Не достаточно хорошо владеет навыками определения угроз безопасности информации и возможные пути противодействия им	На хорошем уровне владеет навыками определения угроз безопасности информации и возможные пути противодействия им	

В рамках рейтинговой системы успеваемость студентов по дисциплине оцениваются знания, умения навыки в ходе текущего контроля и промежуточной аттестации.

Текущий контроль
Рейтинговая оценка знаний студента

№ п/п	Вид деятельности студентов	Сроки выполнения	Количество баллов
	8 семестр		
1.	Выполнение практических работ 1-3	6 неделя	25
2.	Выполнение практических работ 4-6	12 неделя	30
	Итого за 8 семестр		**55**

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

Промежуточная аттестация проводится в форме экзамена

Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если теоретическое содержание курса освоено полностью, без пробелов; исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует в ответе дополнительный материал, все предусмотренные программой задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному; анализирует полученные результаты; проявляет самостоятельность при выполнении заданий.

Оценка «хорошо» выставляется студенту, если теоретическое содержание курса освоено полностью, необходимые практические компетенции в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.

Оценка «удовлетворительно» выставляется студенту, если теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, большинство предусмотренных программой заданий выполнено, но в них имеются ошибки, при ответе на поставленный вопрос студент допускает неточности, недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении программно-го материала.

Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, необходимые практические компетенции не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, качество их выполнения оценено числом баллов, близким к минимальному.

Промежуточная аттестация в форме **экзамена** предусматривает проведение обязательной экзаменационной процедуры и оценивается 40 баллами из 100. Минимальное количество баллов, необходимое для допуска к экзамену, составляет 33 балла. Положительный ответ студента на экзамене оценивается рейтинговыми баллами в диапазоне от **20** до **40** (**20**$\leq S_{экз} \leq$**40**), оценка **меньше 20** баллов считается неудовлетворительной.

Шкала соответствия рейтингового балла экзамена 5-балльной системе

Рейтинговый балл по дисциплине	**Оценка по 5-балльной системе**
35 – 40	Отлично
28 – 34	Хорошо
20 – 27	Удовлетворительно

Итоговая оценка по дисциплине, изучаемой в семестре, определяется по сумме баллов, набранных за работу в течение семестра, и баллов, полученных при сдаче экзамена:

Шкала пересчета рейтингового балла по дисциплине в оценку по 5-балльной системе

Рейтинговый балл по дисциплине	***Оценка по 5-балльной системе***
88 – 100	*Отлично*
72 – 87	*Хорошо*
53 – 71	*Удовлетворительно*
<53	*Неудовлетворительно*

Промежуточная аттестация в форме **курсовой работы.** Максимальная сумма балов по **курсовой работе** устанавливается в **100** балов и переводится в оценку по 5-бальной системе в соответствии со шкалой:

Шкала соответствия рейтингового балла 5-бальной системе

Рейтинговый балл	Оценка по 5-балльной системе
88 – 100	Отлично
72 – 87	Хорошо
53 – 71	Удовлетворительно
<53	*Неудовлетворительно*

8.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этап формирования компетенций

Результатом итоговой проверки знаний студентов по дисциплине учебным планом предусмотрены экзамены.

Вопросы к экзамену (8 семестр)

Вопросы для проверки уровня обученности:

Знать:

1. Что такое управление информационной безопасностью. Основные положения.
2. Управление. Циклическая модель улучшения процессов Основные определения и критерии классификации угроз
3. «Оранжевая книга» как оценочный стандарт.
4. Критерии оценки безопасности информационных систем
5. Стандарты управления информационной безопасностью
6. Этапы создания системы управления ИБ
7. Категорирование активов компании
8. Оценка защищенности информационной системы компании
9. Оценка информационных рисков
10. Управление рисками. Основные понятия.
11. Метод оценки рисков на основе модели угроз и уязвимостей.

Уметь, владеть:

1. 1.Качественные методики управления рисками
2. Количественные методики управления рисками. Метод CRAMM
3. Разработка корпоративной методики анализа рисков. Постановка задачи
4. Методы оценивания информационных рисков
5. Табличные методы оценки рисков
6. Методика анализа рисков Microsoft
7. Обоснование необходимости инвестиций в информационную безопасность компании
8. Современные методы и средства анализа и управление рисками информационных систем компаний. Методика FRAP
9. Современные методы и средства анализа и управление рисками информационных систем компаний. Методика OCTAVE (октэйв)
10. Современные методы и средства анализа и управление рисками информационных систем компаний. Методика RiskWatch (риск вэтч)
11. Протоколирование и аудит. Активный аудит
12. Организационно-правовые формы управления безопасностью
13. Предпосылки развития государственного управления в сфере информационной безопасности

8.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков, характеризующих этапы формирования компетенций

Процедура проведения экзамена осуществляется в соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования в СКФУ. В экзаменационный билет включаются 2 теоретических вопроса. Для подготовки по билету отводится 30 минут.

При подготовке к ответу студенту предоставляется право пользования справочными материалами.

При проверке задания, оцениваются последовательность, рациональность выполнения, точность расчетов, правильность выполнения чертежей и рисунков.

Текущая аттестация студентов проводится преподавателями, ведущими практические по дисциплине, в следующих формах: отчет, собеседование.

Допуск к защите отчетов по практическим работам происходит при наличии у студентов печатного варианта отчета. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. Максимальное количество баллов студент получает, если оформление отчета соответсвует установленным требованиям, а отчет полностью раскрывает суть работы. Основанием для снижением оценки являются:

- частично не соовествует установленным требованиям;
- в отчете непольностью раскрывается суть работы.

Отчет может быть отправлен на доработку в следующих случаях:

- полностью не соовествует установленным требованиям;
- не раскрыта суть работы.

Процедура проведения собеседования проводится в следующей форме: студенту выдается вопрос для собеседования, он готовит ответ (в письменной или устной форме) и отчитывается преподавателю по заданному вопросу. При подготовке к ответу студенту предоставляется право пользования справочными материалами. При проверке задания, оцениваются:

- последовательность и рациональность выполнения;
- точность вычислений;
- знание технологий, использованных при выполнении задания.

Критерии оценивания ответов на вопросы собеседования, отчёта письменного курсовой работе приведены в Фонде оценочных средств по дисциплине «Интегрированные распределенные системы охраны объектов».

9 Методические указания для обучающихся по освоению дисциплины

На первом этапе необходимо ознакомиться с рабочей программой дисциплины, в которой рассмотрено содержание тем дисциплины лекционного курса, взаимосвязь тем лекций с практическими занятиями, темы и виды самостоятельной работы. По каждому виду самостоятельной работы предусмотрены определённые формы отчетности.

Для успешного освоения дисциплины, необходимо выполнить следующие виды самостоятельной работы, используя рекомендуемые источники информации

№ п/п	Виды самостоятельной работы	Рекомендуемые источники информации (№ источника)			
		Основная	Дополнительная	Методическая литература	Интернет-ресурсы
1.	изучение литературы по темам 1-9	1,2	1,2	1-2	1-2
2.	проработка лекционного материала	1,2	1,2	1-2	1-2

3.	подготовка к лабораторным работам	1,2	1,2	1-2	1-2

10. Учебно-методическое и информационное обеспечение дисциплины

10.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины.

10.1.1. Перечень основной литературы:

1. Сергеева Ю.С. Защита информации. Конспект лекций. – М.: А-Приор, 2011.
2. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях - М: ДМК Пресс, 2012. - 596 с.

10.1.2. Перечень дополнительной литературы:

1. Информационная безопасность: учебник для вузов/ В.И. Ярочкин – М.: Академический проект, 2012.
2. Семененко В.А. Информационная безопасность: учеб.пособие/ В.А. Семененко – М.: МГИУ, 2013.

10.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине:

1. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине Интегрированные распределенные системы охраны объектов.
2. Методические указания по выполнению практических работ по дисциплине Интегрированные распределенные системы охраны объектов.

10.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:

1. Университетская библиотека online. http://www.biblioclub.ru.
2. ЭБС «IPRbooks». http://www.iprbookshop.ru.
3. Электронная библиотека СКФУ.. http://catalog.ncstu.ru.
4. Государственная публичная научно- техническая библиотека России. (ГПНТБ России). www.gpntb.ru.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

***Информационные технологии*:**

- Персональные компьютеры, объединенные в локальную сеть и имеющие выход в Интернет;
- Мультимедиа лекции

***Информационные справочные системы*:**

- www.consultant.ru
- www.garant.ru

***Перечень программного обеспечения и информационно-справочных систем*:**

Базовый пакет программ Microsoft Office Standard 2013. Бессрочная лицензия. Дата окончания срока поддержки (обновления) 11.04.2023г., Microsoft Windows Профессиональная. Бессрочная лицензия

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине обеспечение дисциплины

1. Учебная аудитория для проведения занятий лекционного типа: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: проектор, экран

настенный, саб, персональный компьютер. Учебно-наглядные пособия в виде тематических презентаций, соответствующих рабочим программам дисциплин

2. Учебная аудитория для проведения занятий семинарского типа (практических работ): Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, компьютер, проектор, доска магнитно-маркерная Подключение к сети «Интернет», выход в корпоративную сеть университета

3. Учебная аудитория для групповых и индивидуальных консультаций: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, компьютер, проектор, доска магнитно-маркерная Подключение к сети «Интернет», выход в корпоративную сеть университета

4. Учебная аудитория для текущего контроля и промежуточной аттестации: Аудитория, укомплектованная специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории: персональные компьютеры, компьютер, проектор, доска магнитно-маркерная Подключение к сети «Интернет», выход в корпоративную сеть университета