МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное
образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

УТВЕРЖДАЮ
Директор института
Т.А. Шебзухова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Информационная безопасность в системе экономической безопасности

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Специальность	**38.05.01 Экономическая безопасность**
Направленность (профиль)	Финансово-экономическое обеспечение федеральных государственных органов, обеспечивающих безопасность Российской Федерации
Квалификация выпускника	Экономист
Форма обучения	**Очная**
Год начала обучения	**2021 г.**
Изучается в **6** семестре	

Пятигорск, 2021

1. **Цель и задачи освоения дисциплины**

Программа дисциплины «Информационная безопасность в системе экономической безопасности» предназначена для студентов специальности 38.05.01 «Экономическая безопасность».

Цель изучения дисциплины «Информационная безопасность в системе экономической безопасности», изучение комплекса проблем информационной безопасности предпринимательских структур различных типов и направлений деятельности, построения, функционирования и совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сферах охраны интеллектуальной собственности предпринимателей и сохранности, их информационных ресурсов.

Поэтому основными задачами изучения дисциплины являются:

- формирование знаний о концепциях защиты информации и системах безопасности персональных компьютеров и компьютерных сетей;
-изучить теорию и практику новейших достижений и перспектив в развития в области создания систем безопасности локальных вычислительных сетей и сети Internet;
- формирование знаний о криптографических методах зашиты информации; основах криптографии; основных методах и приемах защиты от несанкционированного доступа; о компьютерных вирусах и антивирусных программах; организационно-правовом обеспечение ИБ;
- развитие способности работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации;
- овладение способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;
- формирование навыков выбора инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации и умения обосновывать свой выбор.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность в системе экономической безопасности» относится к базовой части программы, ее освоение происходит в 6 семестре.

3. Связь с предшествующими дисциплинами

Дисциплине «Информационная безопасность в системе экономической безопасности» предшествуют такие дисциплины как «Информатика», «Информационные системы в экономике».

4. Связь с последующими дисциплинами

В свою очередь, овладение знаниями дисциплины «Информационная безопасность в системе экономической безопасности» является необходимым при освоении дисциплины «Мониторинг и прогнозирование рисков и угроз экономической безопасности» и для прохождения практики по получению профессиональных умений и опыта профессиональной деятельности

5. Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

5.1. Наименование компетенций

Код	Формулировка:

ОК-12	способностью работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации
ПК-20	способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности
ПК-29	способностью выбирать инструментальные средства для обработки финансовой, бухгалтерской и иной экономической информации и обосновывать свой выбор

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

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: состав и характеристики современных информационных технологий и ресурсов	ОК-12
Знать: содержание базовых определений и понятий, проблемы информационной безопасности; содержание структур, назначений, особенностей и краткой характеристики функциональных возможностей различных технологий информационной безопасности, организационно-технических, законодательных, программно-аппаратных, математических и т.п. средств их реализации; современное состояние и развитие методов и средств информационной безопасности, методику их применения для решения задач практических задач различного уровня	ПК-20
Знать: состав и функциональные возможности инструментальных средств и информационных технологий обработки информации для решения профессиональных задач экономической безопасности	ПК-29
Уметь: использовать различные информационные ресурсы и технологиями при решении задач экономической безопасности	ОК-12
Уметь: ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области; обосновывать выбор средств для решения конкретных задач информационной безопасности; сводить постановки задач на содержательном уровне к формальным и относить их к соответствующим информационным технологиям; ориентироваться в существующих технологиях информационной безопасности, их возможностях и перспективах развития	ПК-20
Уметь: выявлять угрозы информационной безопасности на основе инструментальной обработки финансовой, бухгалтерской и иной экономической информации	ПК-29
Владеть: навыками работы с различными информационными ресурсами и технологиями	ОК-12
Владеть: навыком анализа информационной инфраструктуры государства и общества; навыком работы с прикладными технологиями, используемыми при проектировании и эксплуатации систем информационной безопасности различных уровней	ПК-20

Владеть: навыками использования инструментальных средств для обеспечения информационной безопасности в системе экономической безопасности	ПК-29

6. Объем учебной дисциплины

	Астр. часов	
Объем занятий: Итого	135 ч.	5 з.е.
В том числе аудиторных	36 ч.	
Из них:		
Лекций	12 ч.	
Практических занятий	24 ч.	
Самостоятельной работы	72 ч.	
Экзамен 6 семестр	27 ч.	

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 (астр.)				Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	
6 семестр							
1	Тема 1. Основные понятия теории информационной безопасности	ОК-12, ПК-20, ПК-29	1,5	3	-	-	
3	Тема 2. Информация как объект защиты	ОК-12, ПК-20, ПК-29	1,5	3	-	-	
5	Тема 3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	ОК-12, ПК-20, ПК-29	1,5	3	-	-	
7	Тема 4. Угрозы информационной безопасности	ОК-12, ПК-20, ПК-29	1,5	3	-	-	
9	Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности	ОК-12, ПК-20, ПК-29	1,5	3	-	-	
11	Тема 6. Построение систем защиты	ОК-12, ПК-20,	1,5	3	-	-	

	от угрозы нарушения целостности информации и отказа доступа	ПК-29					
13	Тема 7. Политика и модели безопасности	ОК-12, ПК-20, ПК-29	1,5	3	-	-	72
15	Тема 8. Обзор международных стандартов информационной безопасности	ОК-12, ПК-20, ПК-29	1,5	3	-	-	
17	Тема 9. Информационные войны и информационное противоборство	ОК-12, ПК-20, ПК-29	-	-	-	-	
Итого за 7 семестр			**12**	**24**	**-**	**-**	**72**
Итого			**12**	**24**	**-**	**-**	**72**

7.2 Наименование и содержание лекций

№ Темы	Наименование тем дисциплины, их краткое содержание	Объем часов (астр.)	Интерактивная форма проведения
6 семестр			
1	**Тема 1. Основные понятия теории информационной безопасности**. История становления теории информационной безопасности. Предметная область теории информационной безопасности. Систематизация понятий в области защиты информации. Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Понятия предметной области «Защита информации». Основные принципы построения систем защиты. Концепция комплексной защиты информации. Задачи защиты информации. Средства реализации комплексной защиты информации.	1,5	
2	**Тема 2. Информация как объект защиты.** Понятие об информации как объекте защиты. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы представления информации. Информационные ресурсы. Структура и шкала ценности информации. Классификация информационных ресурсов. Правовой режим информационных ресурсов.	1,5	
3	**Тема 3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности** Информационная безопасность и ее место в системе национальной безопасности Российской Федерации. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность	1,5	
4	**Тема 4. Угрозы информационной безопасности** Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.	1,5	Лекция-беседа

5	**Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности** Определение и основные способы несанкционированного доступа. Методы защиты от НСД. Организационные методы защиты от НСД. Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация. Основные направления и цели использования криптографических методов. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.	1,5	
6	**Тема 6. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа** Защита целостности информации при хранении. Защита целостности информации при обработке. Защита целостности информации при транспортировке. Защита от угрозы нарушения целостности информации на уровне содержания. Построение систем защиты от угрозы отказа доступа к информации. Защита семантического анализа и актуальности информации.	1,5	
7	**Тема 7. Политика и модели безопасности** Политика безопасности. Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности. Политика и модели дискреционного доступа. Парольные системы разграничения доступа. Политика и модели мандатного доступа. Теоретико-информационные модели. Политика и модели тематического разграничения доступа. Ролевая модель безопасности.	1,5	Лекция-беседа
8	**Тема 8. Обзор международных стандартов информационной безопасности** Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности информационных технологий США. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000.	1,5	
	Итого за 6 семестр	**12**	**3**
	Итого	**12**	**3**

7.3 Наименование лабораторных работ

Данный вид работы не предусмотрен учебным планом

7.4 Наименование практических занятий

№ Темы дисциплины	Наименование тем практических занятий	Объем часов (астр.)	Интерактивная форма проведения

ны			
6 семестр			
1	**Практическое занятие №1.** История становления теории информационной безопасности. Предметная область теории информационной безопасности. Систематизация понятий в области защиты информации.	1,5	
1	**Практическое занятие №2.** Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Понятия предметной области «Защита информации». Основные принципы построения систем защиты. Концепция комплексной защиты информации. Задачи защиты информации. Средства реализации комплексной защиты информации.	1,5	
2	**Практическое занятие №3.** Понятие об информации как объекте защиты. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы представления информации.	1,5	
2	**Практическое занятие №4.** Информационные ресурсы. Структура и шкала ценности информации. Классификация информационных ресурсов. Правовой режим информационных ресурсов.	1,5	
3	**Практическое занятие №5.** Информационная безопасность и ее место в системе национальной безопасности Российской Федерации.	1,5	
3	**Практическое занятие №6.** Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность	1,5	
4	**Практическое занятие №7.** Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз.	1,5	
4	**Практическое занятие №8.** Неформальная модель нарушителя. Оценка уязвимости системы.	1,5	
5	**Практическое занятие №9.** Определение и основные способы несанкционированного доступа. Методы защиты от НСД. Организационные методы защиты от НСД. Инженерно-технические методы защиты от НСД.	1,5	Круглый стол
5	**Практическое занятие №10.** Построение систем защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация. Основные направления и цели использования криптографических методов. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.	1,5	
6	**Практическое занятие №11.** Защита целостности информации при хранении. Защита целостности информации при обработке. Защита целостности информации при транспортировке.	1,5	Круглый стол
6	**Практическое занятие №12.** Защита от угрозы	1,5	

	нарушения целостности информации на уровне содержания. Построение систем защиты от угрозы отказа доступа к информации. Защита семантического анализа и актуальности информации		
7	**Практическое занятие №13.** Политика безопасности. Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности. Политика и модели дискреционного доступа. Парольные системы разграничения доступа.	1,5	Круглый стол
7	**Практическое занятие №14.** Политика и модели мандатного доступа. Теоретико-информационные модели. Политика и модели тематического разграничения доступа. Ролевая модель безопасности.	1,5	
8	**Практическое занятие №15.** Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. Европейские критерии безопасности информационных технологий (ITSEC).	1,5	
8	**Практическое занятие №16.** Федеральные критерии безопасности информационных технологий США. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000.	1,5	
	Итого за 6 семестр	**24**	**4,5**
	Итого	**24**	**4,5**

7.5 Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе (астр.)		
				СРС	Контактная работа с преподавателем	Всего
6 семестр						
ОК-12, ПК-20, ПК-29	Самостоятельное изучение литературы по темам № 6,7,8,9	Конспект	Собеседование	45,8	5,39	53,9
ОК-12, ПК-20, ПК-29	Подготовка к практическим занятиям	Отчет (письменно)	Собеседование	7,29	0,81	8,1
ОК-12, ПК-20, ПК-29	Выполнение индивидуального творческого задания	Отчет (письменно)	Собеседование	9	1	10
			Итого за 6 семестр	**64,8**	**7,2**	**72**
			Итого	**64,8**	**7,2**	**72**
ОК-12, ПК-20, ПК-29	Подготовка к сдаче экзамена	Устный ответ на поставленный вопрос (задание)	Экзамен	**24,3**	**2,7**	**27**

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	Вид контроля, аттестация *(текущий, промежуточный)*	Тип контроля *(устный, письменный или с использованием технических средств)*	Наименование оценочного средства
ОК-12, ПК-20, ПК-29	1-9	собеседование	текущий	Устный, письменный	Вопросы для собеседования
ОК-12, ПК-20, ПК-29	5,6,7	собеседование	текущий	Устный, письменный	Перечень дискуссионных тем для круглого стола
ОК-12, ПК-20, ПК-29	1-9	собеседование	текущий	Устный, письменный	Комплект индивидуальных творческих заданий
ОК-12, ПК-20, ПК-29	1-9	Экзамен	промежуточный	устный	Вопросы к экзамену

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

Уровни сформированности компетенций	**Индикаторы**	**Дескрипторы**			
		2 балла	**3 балла**	**4 балла**	**5 баллов**
ОК-12					
Базовый	**Знать:** состав и характеристики современных информационных технологий и ресурсов	Обучающийся не знает состав и характеристики современных информационных технологий и ресурсов	Имеет слабое ограниченное представление о составе и характеристиках современных информационных технологий и ресурсов	Демонстрирует достаточно полное знание состава и характеристик современных информационных технологий и ресурсов	
	Уметь: использовать различные информационные ресурсы и технологиями при решении задач экономической безопасности	Обучающийся не умеет использовать различные информационные ресурсы и технологиями при решении задач экономической безопасности	Не в полной мере использовать различные информационные ресурсы и технологиями при решении задач экономической безопасности	Демонстрирует умение использовать различные информационные ресурсы и технологиями при решении задач экономической безопасности	
	Владеть: навыками работы с различными информационными ресурсами и технологиями	Обучающийся не владеет навыками работы с различными информационными ресурсами и технологиями	Не в полной мере владеет навыками работы с различными информационными ресурсами и технологиями	Демонстрирует навыки владения навыками работы с различными информационными ресурсами и технологиями	

Повышенный	**Знать:** состав и характеристики современных информационных технологий и ресурсов				Демонстрирует глубокое и прочное знание состава и характеристик современных информационных технологий и ресурсов
	Уметь: использовать различные информационные ресурсы и технологиями при решении задач экономической безопасности				Демонстрирует умение использовать различные информационные ресурсы и технологиями при решении задач экономической безопасности
	Владеть: навыками работы с различными информационными ресурсами и технологиями				Демонстрирует владение навыками работы с различными информационными ресурсами и технологиями
ПК-20					
Базовый	**Знать:** – содержание базовых определений и понятий, проблемы информационной безопасности; – содержание структур, назначений, особенностей и краткой характеристики функциональных возможностей различных технологий информационной безопасности, организационно-технических, законодательных, программно-аппаратных, математических и т.п. средств их реализации	Обучающийся не знает содержание базовых определений и понятий, проблемы информационной безопасности; содержание структур, назначений, особенностей и краткой характеристики функциональных возможностей различных технологий информационной безопасности, организационно-технических, законодательных, программно-аппаратных, математических и т.п. средств их реализации	Имеет слабое ограниченное представление о содержании базовых определений и понятий, проблемы информационной безопасности; содержание структур, назначений, особенностей и краткой характеристики функциональных возможностей различных технологий информационной безопасности, организационно-технических, законодательных, программно-аппаратных, математических и т.п. средств их реализации	Демонстрирует достаточно полное знание содержания базовых определений и понятий, проблемы информационной безопасности; содержание структур, назначений, особенностей и краткой характеристики функциональных возможностей различных технологий информационной безопасности, организационно-технических, законодательных, программно-аппаратных, математических и т.п. средств их реализации	
	Уметь: ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области; обосновывать выбор средств для решения конкретных задач информационной безопасности; ориентироваться в существующих технологиях информационной безопасности, их возможностях и перспективах развития.	Обучающийся не умеет ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области; обосновывать выбор средств для решения конкретных задач информационной безопасности; ориентироваться в существующих технологиях информационной безопасности, их возможностях и перспективах развития.	Не в полной мере может ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области; обосновывать выбор средств для решения конкретных задач информационной безопасности; ориентироваться в существующих технологиях информационной безопасности, их возможностях и перспективах развития.	Демонстрирует умение ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области; обосновывать выбор средств для решения конкретных задач информационной безопасности; ориентироваться в существующих технологиях информационной безопасности, их возможностях и перспективах развития.	
	Владеть: -навыком анализа информационной инфраструктуры государства и общества;	Обучающийся не имеет навыков анализа информационной инфраструктуры государства и	Не в полной мере владеет навыками анализа информационной инфраструктуры государства и общества;	Демонстрирует навыки анализа информационной инфраструктуры государства и общества; - навыком работы с	

	- навыком работы с прикладными технологиями, используемыми при проектировании и эксплуатации систем информационной безопасности различных уровней	общества; - навыком работы с прикладными технологиями, используемыми при проектировании и эксплуатации систем информационной безопасности различных уровней	- навыком работы с прикладными технологиями, используемыми при проектировании и эксплуатации систем информационной безопасности различных уровней	прикладными технологиями, используемыми при проектировании и эксплуатации систем информационной безопасности различных уровней	
Повышенный	**Знать:** – содержание базовых определений и понятий, проблемы информационной безопасности; – содержание структур, назначений, особенностей и краткой характеристики функциональных возможностей различных технологий информационной безопасности, организационно-технических, законодательных, программно-аппаратных, математических и т.п. средств их реализации - современное состояние и развитие методов и средств информационной безопасности, методику их применения для решения задач практических задач различного уровня.				Демонстрирует глубокое и прочное знание содержания базовых определений и понятий, проблемы информационной безопасности; – содержания структур, назначений, особенностей и краткой характеристики функциональных возможностей различных технологий информационной безопасности, организационно-технических, законодательных, программно-аппаратных, математических и т.п. средств их реализации современного состояния и развития методов и средств информационной безопасности, методику их применения для решения задач практических задач различного уровня.
	Уметь: ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области; обосновывать выбор средств для решения конкретных задач информационной безопасности; -сводить постановки задач на содержательном уровне к формальным и относить их к соответствующим информационным технологиям; ориентироваться в существующих технологиях информационной безопасности, их возможностях и перспективах развития.				Демонстрирует умение ориентироваться в области информационной безопасности, пользоваться специальной литературой в изучаемой предметной области; обосновывать выбор средств для решения конкретных задач информационной безопасности; -сводить постановки задач на содержательном уровне к формальным и относить их к соответствующим информационным технологиям; ориентироваться в существующих технологиях информационной безопасности, их возможностях и перспективах развития.
	Владеть: -навыком анализа информационной инфраструктуры				Демонстрирует навыки анализа информационной инфраструктуры

	государства и общества; - навыком работы с прикладными технологиями, используемыми при проектировании и эксплуатации систем информационной безопасности различных уровней				государства и общества; - навыком работы с прикладными технологиями, используемыми при проектировании и эксплуатации систем информационной безопасности различных уровней
ПК-29					
Базовый	**Знать:** Состав и функциональные возможности инструментальных средств и информационных технологий обработки информации для решения профессиональных задач экономической безопасности	Обучающийся не знает состав и функциональные возможности инструментальных средств и информационных технологий обработки информации для решения профессиональных задач экономической безопасности	Обучающийся не в полной мере знает состав и функциональные возможности инструментальных средств и информационных технологий обработки информации для решения профессиональных задач экономической безопасности	Демонстрирует достаточно полное знание состава и функциональных возможностей инструментальных средств и информационных технологий обработки информации для решения профессиональных задач экономической безопасности	
	Уметь: Выявлять угрозы информационной безопасности на основе инструментальной обработки финансовой, бухгалтерской и иной экономической информации;	Обучающийся не умеет выявлять угрозы информационной безопасности на основе инструментальной обработки финансовой, бухгалтерской и иной экономической информации;	Обучающийся не в полной мере умеет выявлять угрозы информационной безопасности на основе инструментальной обработки финансовой, бухгалтерской и иной экономической информации;	Демонстрирует умение выявлять угрозы информационной безопасности на основе инструментальной обработки финансовой, бухгалтерской и иной экономической информации;	
	Владеть: Навыками использования инструментальных средств для обеспечения информационной безопасности в системе экономической безопасности;	Обучающийся не имеет навыков использования инструментальных средств для обеспечения информационной безопасности в системе экономической безопасности;	Не в полной мере владеет навыками использования инструментальных средств для обеспечения информационной безопасности в системе экономической безопасности;	Демонстрирует навыки использования инструментальных средств для обеспечения информационной безопасности в системе экономической безопасности;	
Повышенный	**Знать:** Состав и функциональные возможности инструментальных средств и информационных технологий обработки информации для решения профессиональных задач экономической безопасности				Демонстрирует глубокое и прочное знание состава и функциональных возможностей инструментальных средств и информационных технологий обработки информации для решения профессиональных задач экономической безопасности
	Уметь: Выявлять угрозы информационной безопасности на основе инструментальной обработки финансовой, бухгалтерской и иной экономической информации;				Демонстрирует умение выявлять угрозы информационной безопасности на основе инструментальной обработки финансовой, бухгалтерской и иной экономической информации;
	Владеть: Навыками использования инструментальных средств для				Демонстрирует навыки использования инструментальных средств для обеспечения

	обеспечения информационной безопасности в системе экономической безопасности;				информационной безопасности в системе экономической безопасности;

Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

Рейтинговая оценка знаний студента

№ п/п	Вид деятельности студентов	Сроки выполнения	Количествоб аллов
6 семестр			
1.	Практическое занятие 8	8 неделя	20
2.	Практическое занятие 14	14 неделя	25
	Итого за 6 семестр:		**55**
	Итого:		**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

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** ≤ $S_{экз}$ ≤ **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
< 20	*Неудовлетворительно*

Итоговая оценка по дисциплине, изучаемой в одном 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*

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

Вопросы к экзамену 6 семестр

Вопросы (задача, задание) для проверки уровня обученности

Знать

1. Предметная область теории информационной безопасности.
2. Систематизация понятий в области защиты информации.
3. Основные термины и определения правовых понятий в области информационных отношений и защиты информации.
4. Понятия предметной области «Защита информации».
5. Основные принципы построения систем защиты.
6. Концепция комплексной защиты информации.
7. Задачи защиты информации.
8. Понятие об информации как объекте защиты.
9. Уровни представления информации.
10. Основные свойства защищаемой информации.
11. Виды и формы представления информации.
12. Информационные ресурсы.
13. Классификация информационных ресурсов.
14. Информационная безопасность и ее место в системе национальной безопасности Российской Федерации.
15. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность
16. Анализ уязвимостей системы.
17. Классификация угроз информационной безопасности.
18. Основные направления и методы реализации угроз.
19. Неформальная модель нарушителя.
20. Оценка уязвимости системы.
21. Определение и основные способы несанкционированного доступа.
22. Методы защиты от НСД.
23. Организационные методы защиты от НСД.
24. Инженерно-технические методы защиты от НСД.
25. Построение систем защиты от угрозы утечки по техническим каналам.
26. Идентификация и аутентификация.
27. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.
28. Защита целостности информации при хранении.
29. Защита целостности информации при обработке.
30. Защита целостности информации при транспортировке.
31. Защита от угрозы нарушения целостности информации на уровне содержания.
32. Построение систем защиты от угрозы отказа доступа к информации.
33. Защита семантического анализа и актуальности информации.
34. Политика безопасности.
35. Субъектно-объектные модели разграничения доступа.
36. Аксиомы политики безопасности.
37. Политика и модели дискреционного доступа.

38. Парольные системы разграничения доступа.
39. Политика и модели мандатного доступа.
40. Теоретико-информационные модели.
41. Политика и модели тематического разграничения доступа.
42. Ролевая модель безопасности.
43. Роль стандартов информационной безопасности.
44. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC.
45. Европейские критерии безопасности информационных технологий (ITSEC).
46. Федеральные критерии безопасности информационных технологий США.
47. Единые критерии безопасности информационных технологий.
48. Группа международных стандартов 270000.
49. Определение и основные виды информационных войн.
50. Информационно-техническая война.
51. Информационно-психологическая война.

Уметь, владеть
52. Проанализируйте историю становления теории информационной безопасности
53. Охарактеризуйте средства реализации комплексной защиты информации.
Изобразите схематично структуру и шкалу ценности информации.
54. Проанизируйте правовой режим информационных ресурсов.
55. Оцените место информационной безопасности в системе национальной безопасности Российской Федерации
Изобразите схематично структуру государственной системы защиты информации
56. Определите перечень основных угроз для АС, состоящей из автономно работающего компьютера без выхода в сеть, расположенной в одной из лабораторий университета.
57. Постройте неформальную модель нарушителя для учебной компьютерной лаборатории.
58. Выведите формулу для расчета прочности трехуровневой защитной оболочки.
59. Охарактеризуйте защитные оболочки и перечень преград, применяемые в учебной компьютерной лаборатории.
60. Выявите основные направления и цели использования криптографических методов.
61. Охарактеризуйте основные способы несанкционированного доступа
62. Основные направления и цели использования криптографических методов.
63. Проведите сравнительный анализ обычной и цифровой подписей
64. Составьте схему контроля целостности данных при транспортировке
65. Составьте матрицу доступа и граф доступа для организации документооборота факультета (объекты доступа: экзаменационные ведомости, персональные данные студентов, рабочие программы дисциплин; субъекты доступа: студенты, преподаватели, декан).
63. Оцените роль моделей разграничения доступа в теории информационной безопасности
64. Выявите основные достоинства и недостатки дискреционных моделей
65. Приведите примеры использования дискреционных моделей разграничения доступа.
66. Опишите структуру Общих критериев безопасности информационных технологий.
67. Опишите технологию применения Общих критериев безопасности информационных технологий.
68. Проведите сравнительный анализ «информационной войны» и «информационного противоборства»
69. Составьте схему ведения информационной войны
70. Приведите пример межкорпоративной информационной войны.
71. Выявите особенности информационно-психологической войны

8.4 Методические материалы, определяющие процедуры оценивания знаний, умений,

навыков и (или) опыта деятельности, 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 – программам бакалавриата, программам специалитета, программам магистратуры - в СКФУ. В экзаменационный билет включаются : два вопроса для базового уровня и третий вопрос для повышенного уровня. В билете отмечены * вопросы для повышенного уровня.

Для подготовки по билету отводится 30 минут.

При подготовке к ответу студенту предоставляется право пользования справочными таблицами.

Текущий контроль студентов проводится преподавателем, ведущим лекционные и практические занятия по дисциплине. К практическому занятию студент должен подготовить ответы на вопросы, выполнить задания по теме занятия. Максимальное количество баллов студент получает, если он активно участвует в работе, владеет материалом, умеет логично и четко излагать мысли, творчески подходит к решению основных вопросов темы, показывает самостоятельность мышления.

Основанием для снижением оценки являются:

- слабое знание темы и основной терминологии;
- пассивность участия в групповой работе;
- отсутствие умения применить теоретические знания для решения практических задач;
- несвоевременность предоставления выполненных работ.

Критерии оценивания сформированности компетенций и результатов самостоятельной работы приведены в Фонде оценочных средств по дисциплине «Информационная безопасность в системе экономической безопасности».

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	Дополни-тельная	Методи-ческая	Интернет-ресурсы
1	Самостоятельное изучение литературы по темам № 6,7,8,9	1,2	1-2	1,2	1-5
2	Подготовка к практическим занятиям	1,2	1-2	1,2	1-5
3	Выполнение индивидуального творческого задания	1,2	1-2	1,2	1-5
4	Подготовка к экзамену	1,2	1-2	1,2	1-5

10. Учебно-методическое и информационное обеспечение дисциплины

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

10.1.1. Перечень основной литературы:

1.Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 с. — ISBN 978-5-4487-0585-4. — Текст :

электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86938.html
2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/87995.html

10.1.2. Перечень дополнительной литературы:
1. Информационная безопасность : лабораторный практикум / составители Т. Н. Катанова, Л. С. Галкина, Р. А. Жданов. — Пермь : Пермский государственный гуманитарно-педагогический университет, 2018. — 86 с. — ISBN 978-5-85219-007-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/86357.html.
2.Басыня, Е. А. Системное администрирование и информационная безопасность : учебное пособие / Е. А. Басыня. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с. — ISBN 978-5-7782-3484-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/91423.html

10.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине
1..Методические указания по выполнению практических работ по дисциплине «Информационная безопасность в системе экономической безопасности» для студентов специальности 38.05.01 «Экономическая безопасность», 2020 г.
2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине «по дисциплине «Информационная безопасность в системе экономической безопасности» для студентов специальности 38.05.01 «Экономическая безопасность», 2020 г.

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

Интернет-ресурсы:
1. https://www.zakonrf.info/ - Кодексы и законы - правовая навигационная система.
2. http://pravo.gov.ru/ - официальный интернет портал правовой информации

Электронные библиотечные системы:
3. http://biblioclub.ru/ - Университетская библиотека ONLINE
4. http://www.iprbookshop.ru – Электронная библиотечная система «IPRbooks»

Профессиональные базы данных:
5. http://www.minsvyaz.ru - Официальный сайт Министерства связи и массовых коммуникаций РФ

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

Информационные справочные системы:
1. Справочно-правовая система **Консультант Плюс.**

Программное обеспечение
Microsoft Windows 7 Профессиональная
Microsoft Office

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

Аудитория для проведения лекционных занятий: учебная мебель, доска магнитно-маркерная 1-элементная 120*240, мультимедиа-проектор Epson, персональный компьютер Компьютер - Celeron430/1GB/160GB/DVDROM (10 шт.), Коммутатор - D-LinkDES-1016D (1 шт.), Плата- Secret Net TMCard PCI (10 шт.), Считыватель для Secret Net TMCard (1 шт.), Идентификатор ibutton DS1992 (15 шт.), Аппаратно-программный комплекс HSEC-3.5-IPC25-2P-FW Континент 3,5 Крипто Шлюз (1 шт.), Индикатор поля SEL SP-75Карточка (4 шт.), Ключ активации на использование прогр. прод. Средство управления системой защиты информации (2 шт.), Микроконтроллер - портативный многотерминальный лабораторный комплекс «программируемые микроконтроллеры семейства AVR» (Учебный лабораторный комплекс "Программирование микроконтроллеров AT90S8535 и управление технол. объектами по обучению) (1 шт.), Электронный замок - Соболь для шины в комплекте с идентификаторами (1 шт.)., Учебно-наглядные пособия в виде тематических презентаций, соответствующих рабочим программам дисциплин.

Аудитория для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации: учебная мебель, доска магнитно-маркерная 1-элементная 120*240, мультимедиа-проектор Epson, учебно-наглядные пособия, Генератор шума по сети электропитания и линиям заземления «Соната – РС 1» (1 шт.), Генератор шума ГШ-2500 (1 шт.), Устройство комбинированной защиты объектов информатизации от утечки информации за счет ПЭМИН “Соната-РК1” (1 шт.), Электронно-оптическое устройство «Оптик» (1 шт.) Скоростной поисковый приемник «Скорпион v.34» (1 шт.) Генератор-излучатель виброакустического шума «СВ-45/М» (2 шт.), Портативный металлодетектор «Сфинкс» «ВМ – 612» (в составе: аккумулятор, ЗУ, виброиндикация) (2 шт.) Имитатор закладных устройств «Шиповник-2» (1 шт.), "ИМФ-2" - (2 шт.), ИМФ-3 (1 шт.), ИМф-3-1 (1 шт.), Стенд лабораторный ПКП Magnum Alert+клавиатура» (1 шт.), Стенд лабораторный ПКП Summit 3208+клавиатура» (1 шт.), Стенд лабораторный «ПКП 9234+» (1 шт.), Автоматизированный комплекс «Сигурд-М19» (1 шт.), Комплект дополнительного оборудования для системы Сигурд-М19 (1 шт.), Комплект учебно-методических пособий (1 шт.), Стол поворотный диэлектрический управляемый СПДУ-1 (1 шт.), Короткофокусный мультимедиа-проектор Epson EB-436Wi с настенным креплением и набором кабелей (1 шт.), Комплекс оценки защищенности выделенных помещений по виброакустическому каналу «Шепот» (1 шт.), Цифровой осциллограф "АОС-5302" (1 шт.), Автоматизированный комплекс «Талис-НЧ-М1» (1 шт.), Учебный лабораторный стенд Основы цифровой электроники и микропроцессорной техники с ПЭВМ и осциллографом НТЦ-02.58 (1 шт.). Аудитория подключена к сети «Интернет».

Помещение для самостоятельной работы: учебная мебель, доска кл. 3-х створчатая, компьютер в сборе -16 шт., Аудитория подключена к сети «Интернет», имеется доступ к электронным библиотечным системам и электронной информационно-образовательной среде университета.

13. Особенности освоения дисциплины лицами с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (помощника), оказывающего обучающимся необходимую техническую помощь,а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а так же в отдельных группах.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития,

индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины (модуля) обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),
- письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,
- специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),
- индивидуальное равномерное освещение не менее 300 люкс,
- при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;

2) для лиц с ограниченными возможностями здоровья по слуху:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),
- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;
- обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата (в том числе с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей)

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;
- по желанию студента задания могут выполняться в устной форме