

Федеральное государственное образовательное бюджетное
учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
Омский филиал Финуниверситета
Кафедра «Естественно-научные и гуманитарные дисциплины»

УТВЕРЖДАЮ
Директор Омского филиала
Финуниверситета
 Т.В.Ивашкевич
«16» мая 2025 г.

ПРИЛОЖЕНИЕ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ
УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Год утверждения программы: 2025

Разработчики рабочей программы дисциплины: Велигура А.Н.

НАПРАВЛЕНИЕ **ПОДГОТОВКИ:** 38.03.05 «Бизнес-информатика»,
Образовательная программа «Цифровая
трансформация управления бизнесом: ИТ-
менеджмент в бизнесе»

Составитель актуализации: Шамис В.А.

*Рекомендовано Ученым советом Омского филиала Финуниверситета
(протокол от «16» мая 2025 г. №23)*

*Одобрено кафедрой «Естественно-научных и гуманитарных дисциплин»
(протокол от «30» апреля 2025 г. №4)*

Омск 2025

Приложение к программе дисциплины разработал: кандидат
психологических наук, доцент ***В.А.Шамис***

Управление информационной безопасностью. Приложение к рабочей
программе дисциплины для студентов, обучающихся по направлению
подготовки 38.03.05 «Бизнес-информатика». – Омск, 2025. - 25 стр.

© Омский филиал Финансового университета
при Правительстве Российской Федерации,
2025

4. Объем дисциплины в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся (в семестре, в сессию)	4
5.2 Учебно-тематический план.....	4
5.3. Содержание практических и семинарских занятий	6
6.Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы.....	7
6.2. Методическое обеспечение для аудиторной и внеаудиторной самостоятельной работы	8
7.Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине	8
7.1 Перечень компетенций, формируемых в процессе освоения дисциплины	8
7.2Показатели и критерии оценивания компетенций	9
7.3 Типовые контрольные задания или иные материалы для оценки знаний, умений, владений	15
7.4.Методические материалы, определяющие процедуру оценивания знаний, умений, владений	22
8.Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины.....	22
9.Перечень ресурсов информационно-телекоммуникационной сети_«Интернет», необходимых для освоения дисциплины	23
10.Методические указания для обучающихся по освоению дисциплины.....	23
11.Перечень информационных технологий, используемых при_осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных_справочных систем	25
12.Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине	25

4. Объем дисциплины в зачетных единицах и в академических часах с выделением объема аудиторной (лекции, семинары) и самостоятельной работы обучающихся (в семестре, в сессию)

Трудоемкость дисциплины составляет 3 зачетные единицы. Виды учебной работы (в часах) представлены в таблице.

Вид учебной работы	Всего	Семестр 2
Общая трудоемкость дисциплины	108 (3 з.е.)	108
<i>Аудиторные занятия</i>	50	50
лекции	16	16
практические или семинарские занятия	34	34
<i>Самостоятельная работа</i>	58	58
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	экзамен	экзамен

5.2 Учебно-тематический план

№ п/п	Название темы (раздела) дисциплины	Трудоемкость в часах					Формы текущего контроля успеваемости
		Всего	Аудиторная работа				
			Общая	Лекции и	Практическое занятия		
1	Общие вопросы управления ИБ организации	22	8	4	4	14	Аудиторная работа на семинарских занятиях, доклад, презентация Участие в дискуссии.
2	Специальные вопросы управления ИБ организации	28	14	4	10	14	

3	Реализация системы управления ИБ организации.	28	14	4	10	14	
4	Внутренние нормативные документы по управлению ИБ организации.	30	14	4	10	16	
	Итого:	108	50	16	34	58	
					68%		

5.3. Содержание практических и семинарских занятий

№ п/п	Наименование темы (раздела) дисциплины	Содержание практического занятия	Вопросы к практическому занятию
1	Общие вопросы управления ИБ организации	Роль стандартов в управлении ИБ. Основные организации, издающие стандарты по вопросам управления ИБ. Комплекс стандартов и рекомендаций Банка России по управлению ИБ. Общие требования к системам менеджмента ИБ. <i>Рекомендуемая литература:</i> 8:1-7; 9-12;9	Групповые дискуссии презентация основных подходов. Учебное задание: сравнение подходов к управлению ИБ в ISO, России, США и Германии.
2	Специальные вопросы управления ИБ организации	Управление информационной безопасностью финансовых организаций. Требования и рекомендации Банка России и других регуляторов в сфере управления ИБ финансовых организаций. Комплекс СТО и РСБР ИББС. ГОСТ Р 57580.1 и 57580.2. Вопросы ИБ индустрии платежных карт. Отдельные направления менеджмента ИБ. Обеспечение непрерывности деятельности и восстановления после прерываний. <i>Рекомендуемая литература:</i> 8:1-7; 9-12;9	Групповые дискуссии презентация основных подходов. Учебное задание: Исследование методики ГОСТ Р 57580.2
3	Реализация системы управления ИБ организации.	Планирование в управлении ИБ. Внедрение системы управления ИБ. Анализ системы управления ИБ. Совершенствование системы управления ИБ организации. <i>Рекомендуемая литература:</i> 8: 9-12;9	Групповые дискуссии презентация основных подходов. Учебное задание: Исследование методики оценки модели угроз
4	Внутренние нормативные документы по управлению ИБ организации.	Иерархия внутренних нормативных документов по управлению информационной безопасностью. Требования к организации документационного обеспечения управления информационной безопасностью. Политика информационной безопасности организации. Другие документы по управлению ИБ. Изучение примеров работы с форматами CSV, XML, XHTML, HTML, JSON при помощи Библиотек на языке Python, проектирование собственного приложения, работающего с одним из данных форматов. <i>Рекомендуемая литература:</i> 8:1-7; 9-12;9	групповые дискуссии презентация основных подходов. Учебное задание: Пример составления частных политик

6. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

6.1. Формы внеаудиторной самостоятельной работы

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Общие вопросы управления ИБ организации	Стандарты систем менеджмента качества в управлении ИБ	- работа с учебной, научной и справочной литературой; конспект; подготовка сообщений по теме; подготовка презентаций по теме; выполнение учебного задания
Специальные вопросы управления ИБ организации	Положения ГОСТ Р 57580.1 в документах Банка России. Менеджмент инцидентов ИБ. Обеспечение непрерывности деятельности и восстановления после прерываний.	- работа с учебной, научной и справочной литературой; конспект; подготовка сообщений по теме; подготовка презентаций по теме; выполнение учебного задания
Реализация системы управления ИБ организации.	Определение подхода к оценке риска в организации. Управление ресурсами системы управления ИБ организации. Измерение результативности мер управления для проверки соответствия требованиям ИБ.	- работа с учебной, научной и справочной литературой; конспект; подготовка сообщений по теме; подготовка презентаций по теме; выполнение учебного задания
Внутренние нормативные документы по управлению ИБ организации.	Частные политики ИБ, их назначение и состав.	- работа с учебной, научной и справочной литературой; конспект; подготовка сообщений по теме; подготовка презентаций по теме; выполнение учебного задания

6.2. Методическое обеспечение для аудиторной и внеаудиторной самостоятельной работы

Пример варианта самостоятельной работы

1. Национальная платежная система, ее участники и требования к обеспечению ИБ.
2. Менеджмент инцидентов ИБ.
3. Управление в инфраструктуре открытых ключей.
4. Мошеннические операции в кредитно-финансовой сфере.
5. Аудит ИБ

Примерные темы контрольных работ.

1. Виды информации, подлежащей защите в РФ.
2. Оценка соответствия требованиям ИБ в КФО.
3. Профили защиты.
4. Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и не кредитных финансовых организаций
5. Ключевые требования к защите информации при осуществлении переводов денежных средств.
6. Методика оценки модели угроз и ее применение.
7. Ключевые субъекты НПС.

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

7.1 Перечень компетенций, формируемых в процессе освоения дисциплины

Перечень компетенций, формируемых в процессе освоения дисциплины, содержится в разделе 2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

7.2. Показатели и критерии оценивания компетенций

Зачет по дисциплине выставляется студенту при условии сформированности по каждой компетенции как минимум порогового уровня.

Показатели и критерии оценивания компетенций, описание шкал оценивания

Результаты обучения по дисциплине (модулю)	Шкала и критерии оценки результатов			
	Высокий уровень(отлично)	Продвинутый уровень(хорошо)	Пороговый уровень(удовлетворительно)	Пороговый уровень не достигнут(неудовлетворительно)
ПКН-12 Способность применять вычислительное оборудование, системы хранения данных и инфраструктурные решения центров обработки данных				
<i>1.Проводит анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.</i>				
Знает способы анализа рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Знает отлично способы анализа рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Знает хорошо способы анализа рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Знает удовлетворительно способы анализа рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Не знает способы анализа рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.
Умеет проводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Умеет отлично проводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Умеет хорошо проводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Умеет удовлетворительно проводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Не умеет проводить анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.
<i>2.Консультирует по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.</i>				

Знать основные варианты использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Знает отлично основные варианты использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Знает основные варианты использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Знает некоторые варианты использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Не знает основные варианты использования вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.
Уметь формулировать предложения по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Умеет формулировать предложения по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных; решать нетипичные задачи	Умеет формулировать предложения по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Умеет в некоторой степени формулировать предложения по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	Не умеет формулировать предложения по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных
УК-7 Способность создавать и поддерживать безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий и военных конфликтов				
<i>1.Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда</i>				
Знает: основные требования к технике безопасности на рабочем месте, безопасным условиям труда.	Знает отлично основные требования к технике безопасности на рабочем месте, безопасным условиям труда.	Знает основные требования к технике безопасности на рабочем месте, безопасным условиям труда.	Знает некоторые требования к технике безопасности на рабочем месте, безопасным условиям труда.	Не знает основные требования к технике безопасности на рабочем месте, безопасным условиям труда.
Умеет: выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда	Умеет выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда; решать нетипичные задачи	Умеет выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда.	Умеет в некоторой степени выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда	Не умеет выявлять и устранять проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда

<i>2. Осуществляет выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.</i>				
Знать основные мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.	Знает отлично основные мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.	Знает основные мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.	Знает некоторые мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.	Не знает основные мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.
Уметь проводить мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.	Умеет проводить мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах; решать нетипичные задачи	Умеет проводить мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.	Умеет в некоторой степени проводить мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.	Не умеет проводить мероприятия по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах.
<i>3. Находит пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества</i>				
Знать основные проблемные ситуации, связанные с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества.	Знает отлично основные проблемные ситуации, связанные с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества.	Знает основные проблемные ситуации, связанные с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества.	Знает некоторые проблемные ситуации, связанные с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества.	Не знает основные проблемные ситуации, связанные с безопасностью жизнедеятельности людей, сохранением природной среды, обеспечением устойчивого развития общества.
Уметь находить пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества.	Умеет находить пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества; решать нетипичные задачи	Умеет находить пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества.	Умеет в некоторой степени находить пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества.	Не умеет находить пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества.
<i>4. Действует в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания</i>				

Знать основные способы выживания в экстремальных и чрезвычайных ситуациях.	Знает отлично основные способы выживания в экстремальных и чрезвычайных ситуациях	Знает основные способы выживания в экстремальных и чрезвычайных ситуациях	Знает некоторые способы выживания в экстремальных и чрезвычайных ситуациях	Не знает основные способы выживания в экстремальных и чрезвычайных ситуациях
Уметь применять на практике основные способы выживания.	Умеет применять на практике основные способы выживания; решать нетипичные задачи	Умеет применять на практике основные способы выживания.	Умеет в некоторой степени применять на практике основные способы выживания.	Не умеет применять на практике основные способы выживания.

Текущий контроль осуществляется в ходе учебного процесса и консультирования студентов, по результатам выполнения проектов на практических занятиях и самостоятельно с использованием компьютерных технологий моделирования бизнес-процессов предприятия и системного анализа, а также компьютерного тематического тестирования.

Основными формами текущего контроля знаний являются:

решение прикладных задач средствами профессионально-ориентированных информационных систем и технологий, уяснение эффективных подходов к выбору инструментальных средств и их применению в различных проблемных ситуациях;

проверка качества усвоения проблемных вопросов изучаемого материала в ходе плановых занятий, обсуждение на семинарах контрольных вопросов, вынесенных в планы;

поисково-аналитическая работа по сбору и анализу материала по тематике внеаудиторной расчетно-аналитической работы, его обработка, формирование отчета, представление и публичная защита результатов;

проверка соответствия разработки электронных деловых документов установленным требованиям стандартов, правильности выбора и полноты использования средств информационных технологий;

выполнение контрольных работ и самостоятельных заданий, их оценивание и обсуждение результатов;

компьютерное тематическое тестирование по теоретическим и практическим вопросам дисциплины.

Промежуточная аттестация студентов по дисциплине «Управление информационной безопасностью» проводится в форме зачета.

Текущий контроль осуществляется в ходе учебного процесса и консультирования студентов, а также на основе результатов выполнения самостоятельных работ. На контроль выносятся:

- вопросы, вынесенные на самостоятельное изучение и осмысление,

- вопросы и тесты на освоение минимально необходимого материала,
- решения индивидуальных задач с позиций системной методологии при написании доклада.

Оценка знаний по 100-бальной шкале проводится в соответствии с нормативными документами Финуниверситета

№ п/п	Вид отчетности	Баллы всего
1.	Текущий контроль	40
	Активное участие в семинарах, посещаемость	10
	Домашняя контрольная работа	5
	Аудиторная контрольная работа	10
	Итоговая контрольная работа	15
2.	Экзамен	60
3.	Итого	100

7.3 Типовые контрольные задания или иные материалы для оценки знаний, умений, владений

Промежуточная аттестация проводится в форме зачета.

Компетенция	Индикаторы достижения компетенции	Вопросы к зачету, Тестовые задания, Практико-ориентированные задания
ПKN-12 Способность применять вычислительное оборудование, системы хранения данных и инфраструктурные решения центров обработки данных	1. Проводит анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Вопросы к зачету: 1. В чем основное отличие информационной безопасности от киберустойчивости? 2. Укажите основные государственные органы, требования которых по защите информации обязательны. 3. Что такое угроза (ИБ)? 4. Что такое уязвимость (в контексте ИБ) и к чему она относится? Тестовые задания: 1. Под информационной безопасностью понимается... А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре. Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия В) нет правильного ответа 2. Защита информации – это.. А) комплекс мероприятий, направленных на обеспечение информационной безопасности. Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей В) небольшая программа для выполнения определенной задачи 3. От чего зависит информационная безопасность? А) от компьютеров Б) от поддерживающей инфраструктуры В) от информации 4. Основные составляющие информационной безопасности: А) целостность

	Б) достоверность В) конфиденциальность 5. Доступность – это... А) возможность за приемлемое время получить требуемую информационную услугу. Б) логическая независимость В) нет правильного ответа 6. Целостность – это.. А) целостность информации Б) непротиворечивость информации В) защищенность от разрушений 7. Конфиденциальность – это.. А) защита от несанкционированного доступа к информации Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов В) описание процедур <i>Практико-ориентированные задания</i> 1. Составить аналитический обзор инфраструктурных решений центров обработки данных
2. Консультирует по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных.	<i>Вопросы к зачету:</i> 1. Какие виды информации подлежат защите в соответствии с нормативными актами госрегуляторов? 2. В чем заключаются особенности защиты коммерческой тайны? 3. Что такое инсайдерская информация с точки зрения закона «О противодействии правонарушению использованию инсайдерской информации...» (224-ФЗ)? 4. Какие вопросы защиты информации в негосударственной сфере регулирует ФСБ? <i>Тестовые задания:</i> 1. Какие трудности возникают в информационных системах при конфиденциальности? А) сведения о технических каналах утечки информации являются закрытыми Б) на пути пользовательской криптографии стоят многочисленные

		технические проблемы В) все ответы правильные 2. Угроза – это... А) потенциальная возможность определенным образом нарушить информационную безопасность Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа 3. Атака – это... А) попытка реализации угрозы Б) потенциальная возможность определенным образом нарушить информационную безопасность В) программы, предназначенные для поиска необходимых программ. 4. Источник угрозы – это.. А) потенциальный злоумышленник Б) злоумышленник В) нет правильного ответа 5. Окно опасности – это... А) промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется. Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере 6. Какие события должны произойти за время существования окна опасности? А) должно стать известно о средствах использования пробелов в защите. Б) должны быть выпущены соответствующие заплатки. В) заплатки должны быть установлены в защищаемой И.С. 7. Угрозы можно классифицировать по нескольким критериям: А) по спектру И.Б. Б) по способу осуществления
--	--	--

		В) по компонентам И.С. 8. По каким компонентам классифицируются угрозы доступности: А) отказ пользователей Б) отказ поддерживающей инфраструктуры В) ошибка в программе <i>Практико-ориентированные задания</i> 1. Изложить варианты сегментации вычислительного оборудования центров обработки данных согласно требованиям к защите информации финансовых организаций.
УК-7 Способность создавать и поддерживать безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий и военных конфликтов	1. Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда	<i>Вопросы к зачету:</i> 1. Какие виды информации подлежат защите в соответствии с нормативными актами госрегуляторов? 2. На какие категории подразделяются персональные данные? 3. Что такое банковская тайна? 4. Какие вопросы защиты информации в негосударственной сфере регулирует ФСТЭК? <i>Тестовые задания:</i> 1. Основными источниками внутренних отказов являются: А) отступление от установленных правил эксплуатации Б) разрушение данных В) все ответы правильные 2. Основными источниками внутренних отказов являются: А) ошибки при конфигурировании системы Б) отказы программного или аппаратного обеспечения В) выход системы из штатного режима эксплуатации 3. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы: А) невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности Б) обрабатывать большой объем программной информации В) нет правильного ответа 4. Какие существуют грани вредоносного П.О.? А) вредоносная функция Б) внешнее представление

		В) способ распространения 5. По механизму распространения П.О. различают: А) вирусы Б) черви В) все ответы правильные 6. Вирус – это... А) код обладающий способностью к распространению путем внедрения в другие программы Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов В) небольшая программа для выполнения определенной задачи 7. Черви – это... А) код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения Б) код обладающий способностью к распространению путем внедрения в другие программы В) программа действий над объектом или его свойствами 8. Конфиденциальную информацию можно разделить: А) предметную Б) служебную В) глобальную 9. Природа происхождения угроз: А) случайные Б) преднамеренные В) природные 10. Предпосылки появления угроз: А) объективные Б) субъективные В) преднамеренные <i>Практико-ориентированные задания</i> Составить план контроля соблюдения техники безопасности на рабочем месте
--	--	--

	2. Осуществляет выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях и военных конфликта	<i>Вопросы к зачету:</i> 1. Что такое идентификация и аутентификация? 2. Укажите типы факторов аутентификации. 3. Опишите основные угрозы аутентификации. 4. Укажите плюсы и минусы парольной аутентификации. <i>Тестовые задания:</i> 1. К какому виду угроз относится присвоение чужого права? А) нарушение права собственности Б) нарушение содержания В) внешняя среда 2. Отказ, ошибки, сбой – это: А) случайные угрозы Б) преднамеренные угрозы В) природные угрозы 3. Отказ - это... А) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций Б) некоторая последовательность действий, необходимых для выполнения конкретного задания В) структура, определяющая последовательность выполнения и взаимосвязи процессов 4. Ошибка – это... А) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций В) негативное воздействие на программу <i>Практико-ориентированные задания</i> Составить проект мероприятий по действиям в чрезвычайных ситуациях
--	---	--

	3.Находит пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества.	<i>Тестовые задания</i> 1.Сбой – это... А) такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния В) объект-метод 2.Побочное влияние – это... А) негативное воздействие на систему в целом или отдельные элементы Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций 3.СЗИ (система защиты информации) делится: А) ресурсы автоматизированных систем Б) организационно-правовое обеспечение В) человеческий компонент <i>Практико-ориентированные задания</i> Составить план проведения тренировок по действиям в чрезвычайных ситуациях
	4.Действует в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания	<i>Практико-ориентированные задания</i> Составить проект методических рекомендаций по применению на практике основных способов выживания.

7.4.Методические материалы, определяющие процедуру оценивания знаний, умений, владений

Соответствующие приказы, распоряжения ректората, директора филиала о контроле знаний студентов.

8.Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Нормативные акты

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне».
3. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
5. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
6. Указ Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» (вместе с "Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети "Интернет" и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети "Интернет").
7. Указ Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Основная литература

8. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2022. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/498889>

Дополнительная литература

9. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/496741>
10. Нетёсова, О. Ю. Информационные системы и технологии в экономике:

учебное пособие для вузов / О. Ю. Нетёсова. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 178 с. — (Высшее образование). — ISBN 978-5- 534-08223-4. — Текст : электронный // Образовательная платформа Юрайт [сайт].

— URL: <https://urait.ru/bcode/491479>

11. Чекулаева, Е. Н. Управление информационной безопасностью: учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. — Йошкар-Ола : ПГТУ, 2020. — 154 с.

— ISBN 978-5-8158-2165-1. — Текст : электронный // Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/157473> — Режим доступа: для авториз. пользователей.

11. Толстобров, А. П. Управление данными : учебное пособие для вузов / А. П. Толстобров. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 272 с. — (Высшее образование). — ISBN 978-5-534-14162-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/496748> (дата обращения: 26.06.2022).

12. Шилов, А. К. Управление информационной безопасностью : учебное пособие / А. К. Шилов ; Южный федеральный университет. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 120 с. - ISBN 978-5-9275-2742-7. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1021744>— Режим доступа: по подписке.

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

1. Сайт Центрального банка Российской Федерации: www.cbr.ru.
2. Сайт Федеральной службы по техническому и экспортному контролю: www.fstec.ru.
3. Сайт Федерального агентства по техническому регулированию и метрологии: www.gost.ru.
4. Электронная библиотека Финансового университета (ЭБ) <http://elib.fa.ru/>.
5. Электронно-библиотечная система BOOK.RU <http://www.book.ru>.
6. Электронно-библиотечная система «Университетская библиотека ОНЛАЙН» <http://biblioclub.ru/>.
7. Электронно-библиотечная система Znanium <http://www.znanium.com>.
8. Электронно-библиотечная система издательства «ЮРАЙТ» <https://urait.ru/>
9. Электронно-библиотечная система издательства Проспект <http://ebs.prospekt.org/books>.

10. Методические указания для обучающихся по освоению дисциплины

Изучение дисциплин требует систематического и последовательного накопления знаний, следовательно, пропуски отдельных тем не позволяют глубоко освоить предмет.

Студентам необходимо ознакомиться с содержанием рабочей программы

дисциплины (РПД), с целями и задачами дисциплины, ее связями с другими дисциплинами образовательной программы, методическими разработками по данной дисциплине, имеющимися на образовательном портале и сайте университета, с графиком консультаций преподавателей кафедры.

При подготовке к лекционным занятиям студентам необходимо:

- перед каждой лекцией просматривать РПД, что позволит сэкономить время на записывание темы лекции, ее основных вопросов, рекомендуемой литературы;
- на отдельные лекции приносить соответствующий материал на бумажных носителях, представленный лектором на портале или присланный на «электронный почтовый ящик группы» (таблицы, графики, схемы). Данный материал будет охарактеризован, прокомментирован, дополнен непосредственно на лекции.

В целях успешного овладения дисциплиной, получения соответствующих оценок на семинарских занятиях и на экзамене студенты должны вести регулярную самостоятельную работу по изучению теоретических вопросов, рассматриваемых на лекциях, и по получению навыков самостоятельного практического освоению ключевых проблем принятия и исполнения государственных решений.

Основным назначением семинарских занятий является контроль за ходом выполнения самостоятельной работы, рассмотрение наиболее сложных, спорных вопросов и проблемных практических ситуаций, и тем дисциплины, а также получение навыков решения практических ситуаций и работы с нормативными правовыми актами. Материалы для проведения семинарских занятий содержат нормативные и методические материалы, а также обеспечивают разбор типовых практических задач и примеров, анализ которых позволяет студентам овладеть навыками и приемами их решения.

Кроме рекомендуемой к изучению литературы студенты должны в обязательном порядке регулярно (не реже 1-ого раза в месяц просматривать основные периодические источники, рекомендуемые в списке дополнительной литературы. Кроме того, студенты должны отслеживать появление новых нормативных правовых актов, а также изменения действующих документов в сфере принятия и исполнения государственных решений и сообщать на семинарах об изменениях, появлении интересных, проблемных статей и других значимых событиях. Целесообразно, чтобы студенты знакомились с информацией, размещаемой в специализированных интернет-источниках.

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

Комплект лицензионного программного обеспечения:

1. Astra Linux Special Edition

Современные профессиональные базы данных и информационные справочные системы:

1. Справочная правовая система «КонсультантПлюс» (<http://www.consultant.ru>).
2. Информационно-образовательный портал Финансового университета. - <https://org.fa.ru>, <http://campus.fa.ru>

Сертифицированные программные и аппаратные средства защиты информации – не предусмотрено.

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

Для осуществления образовательного процесса по дисциплине необходимо использовать аудитории, оснащенные компьютерами и проектором для демонстрации презентаций.