

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Б1.В.15
(индекс дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы управления информационной безопасностью
(наименование дисциплины)

по направлению подготовки
09.03.03 Прикладная информатика
направленность (профиль)

Прикладная информатика в информационной безопасности

Форма обучения: очная

Год набора: 2026

Общая трудоемкость: 43Е

Распределение часов дисциплины по семестрам

Семестр	5	Итого
Форма контроля	зачет	
Вид занятий		
Лекции	16	16
Лабораторные	-	-
Практические	32	32
Руководство: курсовые работы (проекты) / РГР	-	-
Промежуточная аттестация	0.25	0.25
Контактная работа	48.25	48.25
Самостоятельная работа	95.75	95.75
Контроль		
Итого	144	144

Рабочую программу составил(и):

доцент ИИиЭБ, к.т.н. Полякова Е.В.

(должность, ученое звание, степень, Фамилия И.О.)

(должность, ученое звание, степень, Фамилия И.О.)

Рецензирование рабочей программы дисциплины:



Отсутствует



Рецензент

(должность, ученое звание, степень, Фамилия И.О.)

Рабочая программа дисциплины составлена на основании ФГОС ВО и учебного плана направления подготовки (специальности) 09.03.03 Прикладная информатика

Срок действия рабочей программы до 31 декабря 2031 года

УТВЕРЖДЕНО

На заседании института инженерной и экологической безопасности

(протокол заседания № 1 от «01» сентября 2025 г.).

1. Цель освоения дисциплины

Целью освоения дисциплины является – изучение основных понятий, методологии и практических приемов управления технической и организационно инфраструктурой обеспечения информационной безопасности в организации, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ).

Основные задачи изучения дисциплины:

- формирование у обучаемых понимания роли процессов управления в обеспечении информационной безопасности организаций, объектов и систем;
- ознакомление обучаемых с основными методами управления информационной безопасностью организаций, объектов и систем, обучение различным методам реализации процессов управления информационной безопасностью, направленных на эффективное управление ИБ конкретной организации;
- приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, организации и разграничения полномочий персонала, ответственного за информационную безопасность.

2. Место дисциплины в структуре ОПОП ВО

Дисциплины и практики, на освоении которых базируется данная дисциплина:

- Организация обработки персональных данных в организации;
- Международные и российские нормативные акты, и стандарты по информационной безопасности.

Полученные знания используются при изучении следующих дисциплин:

- Техническая защита информации;
- Моделирование процессов и средств защиты информации

3. Планируемые результаты обучения

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
ПК-8 Использует знания современных подходов к управлению ИБ и направления их развития, основных стандартов, регламентирующие управление ИБ	ПК-8.1 Использует знания современных подходы к управлению ИБ и направления их развития, основных стандартов, регламентирующие управление ИБ	Знать: <ul style="list-style-type: none">- современные подходы к управлению ИБ и направления их развития;- основные стандарты, регламентирующие управление ИБ;- принципы построения СУИБ; принципы разработки процессов управления ИБ;- взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ;

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
		<p>- подходы к интеграции СУИБ в общую систему управления предприятием</p> <p>Уметь:</p> <ul style="list-style-type: none"> - определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; - применять процессный подход к управлению ИБ в различных сферах деятельности; - используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность; <p>Владеть:</p> <ul style="list-style-type: none"> -навыками управления информационной безопасностью простых объектов; - навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;
	<p>ПК-8.2 Использует знания принципов построения СУИБ и разработки процессов управления ИБ</p> <p>ПК-8.3 Умеет анализировать текущее состояние ИБ на предприятии с целью</p>	<p>Знать:</p> <ul style="list-style-type: none"> - теорию разработки документации по ИБ <p>Уметь:</p> <ul style="list-style-type: none"> -анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; - разрабатывать и внедрять СУИБ и оценивать ее эффективность. <p>Владеть:</p> <ul style="list-style-type: none"> - терминологией и процессным подходом построения систем управления ИБ <p>Знать:</p> <ul style="list-style-type: none"> - правила оформления документации по ИБ <p>Уметь:</p>

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
	разработки требований к разрабатываемым процессам управления ИБ, определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ	<p>- практически решать задачи формализации разрабатываемых процессов управления ИБ;</p> <p>Владеть:</p> <p>- навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом.</p>
	ПК-8.4 Владеет навыками управления информационной безопасностью простых объектов, терминологией и процессным подходом построения систем управления ИБ	<p>Знать:</p> <p>- процессный подход с СМИБ</p> <p>Уметь:</p> <p>- реализовать процессный подход в СМИБ</p> <p>Владеть:</p> <p>- навыками построения процессов СМИБ</p>
ПК-9 Способен формулировать политики информационной безопасности	ПК-9.4 Использует знания федерального законодательства, других руководящих документов при разработке ОРД	<p>Знать:</p> <p>- современные подходы к управлению ИБ и направления их развития;</p> <p>- основные стандарты, регламентирующие управление ИБ;</p> <p>- принципы построения СУИБ; принципы разработки процессов управления ИБ;</p> <p>- взаимосвязи отдельных процессов управления ИБ в рамках общей СУИБ;</p> <p>- подходы к интеграции СУИБ в общую систему управления предприятием</p> <p>Уметь:</p> <p>- определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ;</p> <p>- применять процессный подход к управлению ИБ в различных сферах деятельности;</p> <p>- используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность;</p>

Формируемые и контролируемые компетенции (код и наименование)	Индикаторы достижения компетенций (код и наименование)	Планируемые результаты обучения
		<p>Владеть:</p> <ul style="list-style-type: none"> -навыками управления информационной безопасностью простых объектов; - навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;
	ПК-9.5 Умеет разработать Политику информационной безопасности	<p>Знать:</p> <ul style="list-style-type: none"> - теорию разработки документации по ИБ <p>Уметь:</p> <ul style="list-style-type: none"> -анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; - разрабатывать и внедрять СУИБ и оценивать ее эффективность. <p>Владеть:</p> <ul style="list-style-type: none"> - терминологией и процессным подходом построения систем управления ИБ
	ПК-9.6 Владеет стилистикой оформления документации	<p>Знать:</p> <ul style="list-style-type: none"> - правила оформления документации по ИБ <p>Уметь:</p> <ul style="list-style-type: none"> - практически решать задачи формализации разрабатываемых процессов управления ИБ; <p>Владеть:</p> <ul style="list-style-type: none"> - навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом

4. Структура и содержание дисциплины

Модуль (раздел)	Вид учебной работы	Наименование тем занятий (учебной работы)	Семестр	Объем, ч.	Баллы	Интерактив, ч.	Формы текущего контроля (наименование оценочного средства)
Модуль 1	Лек 1	Тема 1 Основные понятия управления информационной безопасностью Понятие информационной безопасности. Основные составляющие информационной безопасности. Управление информационной безопасностью. Стандарты СМИБ. Понятие СУИБ. Место СУИБ в рамках общей системы управления предприятием. Критерии эффективности СУИБ. Структура и шкала ценности информации. Определение границ системы управления ИБ. Система менеджмента ЗИ. Координация обеспечения ИБ. Положения и принципы СУИБ.	5	2	-	-	Банк тестовых заданий/ Устный опрос
Модуль 1	Пр 1	Тема 1 1 Основные понятия управления информационной безопасностью Определение границ системы управления информационной безопасностью и конкретизация целей ее создания.	5	2	2	-	Практическое задание 1
Модуль 1	Пр 2	Тема 1 1 Основные понятия управления информационной безопасностью Определение границ системы управления информационной безопасностью и конкретизация целей ее создания.	5	2	2	-	Практическое задание 1
Модуль 1	Лек 2	Тема 2 Процессорный подход в управлении ИБ Понятие процесса. Методы формализации процессов. Цели и задачи формализации	5	2	-	-	Банк тестовых заданий/ Устный опрос

		процессов. Понятие процессного подхода. Процессный подход к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления (на примере СУИБ). Аудит ИБ. Оценка соответствия мер защиты требованиям ИБ.					
Модуль 1	Пр 3	Тема 2 Процессорный подход в управлении ИБ Аудит безопасности в соответствии с ГОСТ Р ИСО/МЭК 27001.	5	2	2	-	Практическое задание 2
Модуль 1	Пр 4	Тема 2 Процессорный подход в управлении ИБ Аудит безопасности в соответствии с ГОСТ Р ИСО/МЭК 27001.	5	2	2	-	Практическое задание 2
Модуль 1	Лек 3	Тема 3 Основные процессы СУИБ. Создание СУИБ в организации. Определение целей и задач СУИБ. Процесс «Мониторинг эффективности» Процессы «Управление документами». Процесс «Ответственность руководства». Процесс «Подготовка, осведомленность и квалификация персонала». Процессы «Анализ угроз и рисков». (включая разработку метрик эффективности). Понятие «Зрелость процесса». Политика ИБ. «Анализ со стороны высшего руководства». Принципы СУИБ. Процесс выстраивания культуры ИБ. Недопустимые события. Этапы внедрения. COBIT5.	5	2	-	-	Банк тестовых заданий/ Устный опрос
Модуль 1	Пр 5	Тема 3 Основные процессы СУИБ. Создание СУИБ в организации Практическая разработка процессов СУИБ. Расчет метрик информационной безопасности.	5	2	2	-	Практическое задание 3

Модуль 1	Пр 6	Тема 3 Основные процессы СУИБ. Создание СУИБ в организации Практическая разработка процессов СУИБ. Расчет метрик информационной безопасности.	5	2	2	-	Практическое задание 3
Модуль 1	Лек 4	Тема 4 Современные методы и средства анализа и управление рисками информационных систем. Тренды и проблемы управления рисками. Структура информационного риска. Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Определение угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Метод оценки рисков на основе модели угроз и уязвимостей.	5	2	-	-	Банк тестовых заданий/ Устный опрос
Модуль 1	Пр 7	Тема 4 Современные методы и средства анализа и управление рисками информационных систем Технологии (методики) управления информационными рисками	5	2	2	-	Практическое задание 4
Модуль 1	Пр 8	Тема 4 Современные методы и средства анализа и управление рисками информационных систем Технологии (методики) управления информационными рисками	5	2	2	-	Практическое задание 4
Модуль 1	Лек 5	Тема 5 Эффективное построение ИБ, оценка зрелости процессов ИБ. Методика оценки зрелости процессов ИБ. Домены и направления процессов ИБ. План развития ИБ. Управление инцидентами ИБ.	5	2	-	-	Банк тестовых заданий/ Устный опрос
Модуль 1	Пр 9	Тема 5 Эффективное построение ИБ, оценка зрелости процессов ИБ.	5	2	2	-	Практическое задание 5

		Оценка рисков					
Модуль 1	Пр 10	Тема 5 Эффективное построение ИБ, оценка зрелости процессов ИБ. Оценка рисков	5	2	2	-	Практическое задание 5
Модуль 1	Лек 6	Тема 6 Управление угрозами безопасности информации. БДУ ФСТЭК.. Тактики и техники.. Сравнение тактик и техник. Виды и классификация угроз. Нарушители. Уязвимости. Управление уязвимостями.	5	2	-	-	Банк тестовых заданий/ Устный опрос
Модуль 1	Пр 11	Тема 6 Управление угрозами безопасности информации. Выявление угроз информационной безопасности	5	2	2	-	Практическое задание 6
Модуль 1	Пр 12	Тема 6 Управление угрозами безопасности информации. Выявление угроз информационной безопасности	5	2	2	-	Практическое задание 6
Модуль 1	Лек 7	Тема 7 Экономика защиты информации Система ресурсобеспечения защиты информации и эффективность её использования	5	2	-	-	Банк тестовых заданий/ Устный опрос
Модуль 1	Пр 13	Тема 7 Экономика защиты информации Прогнозирование и планирование затрат на ИБ	5	2	2	-	Практическое задание 7
Модуль 1	Пр 14	Тема 7 Экономика защиты информации Прогнозирование и планирование затрат на ИБ	5	2	2	-	Практическое задание 7
Модуль 1	Лек 8	Тема 8 Некоторые аспекты практической СУИБ. План DRP. Управление персоналом и ИБ. Кадровые решения в организации по информационной безопасности. Безопасность, связанная с персоналом	5	2	-	-	Банк тестовых заданий/ Устный опрос

		Обеспечение ИБ при малом бюджете. Практические вопросы. План DRP					
Модуль 1	Пр 15	Тема 8 Некоторые аспекты практической СУИБ. План DRP. Разработка верхнеуровневых документов по ИБ.	5	2	62		Практическое задание 8
	Ср	Самостоятельное изучение материала, не вошедшего в курс лекций	5	95,75	-	-	Банк тестовых заданий
	ПА	Промежуточная аттестация	5	0,25	-	-	Вопросы к зачету
	Псщ	Посещаемость	5	-	10	-	
	Пр 16	Итоговое тестирование	5	2	100	-	Тестовые задания
Итого:				144			

Схема расчета итогового балла

Обучающийся получает до 90 баллов за выполнение практических заданий, до 10 баллов за посещаемость и проходит итоговое тестирование, оцениваемое от 0 до 100 в зависимости от успешности его прохождения. Итоговый балл за курс рассчитывается, как сумма баллов за выполнение практических заданий, баллов за посещаемость и баллов, набранных в ходе тестирования, после чего вся сумма делится на 2. Бонусные баллы выставляются студенту за участие в олимпиадах, конференциях, форумах.

5. Образовательные технологии

Технология	Формы обучения	Методы обучения
Технология традиционного обучения – организация учебного процесса в вузе, основанная на лекционно-семинарско-зачетной формах обучения	Лекция. Практическое занятие. Самостоятельная работа. Индивидуальное домашнее задание.	Наглядные, словесные, практические.
Технология модульного обучения – организация учебного процесса для полного овладения содержанием образовательных программ на основе независимых учебных модулей с учетом индивидуальных интересов и возможностей субъектов образовательного процесса.	Лекция-консультация. Семинар с использованием метода анализа конкретных ситуаций.	Решение ситуационных задач. Презентационный метод. Самостоятельная работа. Консультация. Индивидуальная работа.
Информационные технологии – специальные способы, программные и технические средства (кино, аудио – и видеосредства, компьютеры) для работы с информацией	Лекция-пресс-конференция. Визуальная лекция.	Презентационный метод.

6. Методические указания по освоению дисциплины

Изучение дисциплины предусматривает чтение лекций, проведение практических занятий, самостоятельное изучение специальной литературы по вопросам лекций.

Изучение теоретического материала определяется рабочей учебной программой дисциплины, включенным в нее перечнем литературы. Рекомендуется при подготовке к занятиям повторить материал предшествующих тем лекций.

При подготовке к практическому занятию необходимо изучить материалы лекции, рекомендованную литературу. Изученный материал следует проанализировать в соответствии с планом занятия, затем проверить степень усвоения содержания вопросов.

Виды самостоятельной работы обучающихся:

1. Повторение пройденного лекционного материала, чтение рекомендованной литературы.

2. Подготовка к практическим занятиям.

3. Работа с электронными источниками.

4. Подготовка к сдаче зачета.

Самостоятельная работа обучающихся заключается в изучении литературы, дополняющей материал, излагаемый в лекционной части курса. Необходимо овладеть навыками библиографического поиска, в том числе в сетевых Интернет-ресурсах, научиться сопоставлять различные точки зрения и определять методы исследований.

При подготовке к зачету следует руководствоваться перечнем вопросов для подготовки к итоговому контролю по курсу. При этом необходимо уяснить суть основных понятий дисциплины.

Предполагается, что, прослушав лекцию, обучающийся должен ознакомиться с рекомендованной литературой из основного списка, осуществить поиск и критическую оценку материала на сайтах Интернет, собрать необходимую информацию

7. Оценочные средства

7.1. Паспорт оценочных средств

Семестр	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
5	ПК-9, ПК-8	Тестовые задания. Вопросы к зачету № 1-60. Практические задания № 1-8

7.2. Типовые задания или иные материалы, необходимые для текущего контроля

7.2.1. Практическое задание

(наименование оценочного средства)

Практическое задание 1. Определение границ системы управления информационной безопасностью и конкретизация целей ее создания.

Практическое задание 2. Аудит безопасности в соответствии с ГОСТ Р ИСО/МЭК 27001.

Практическое задание 3. Практическая разработка процессов СУИБ. Расчет метрик информационной безопасности.

Практическое задание 4. Технологии (методики) управления информационными рисками

Практическое задание 5. Оценка рисков

Практическое задание 6. Выявление угроз информационной безопасности

Практическое задание 7. Прогнозирование и планирование затрат на ИБ

Практическое задание 8. Разработка верхнеуровневых документов по ИБ

Типовой(ые) пример(ы) задания(ий)

Цель: Сформировать навыки определения области применения системы управления информационной безопасностью, анализа контекста организации и формулирования измеримых целей защиты информации, согласованных с бизнес-стратегией.

Задание:

1. Студент анализирует профиль условной или реальной организации, выявляет ключевые бизнес-процессы, критические информационные активы, вовлечённые подразделения, технологические платформы и географические локации.
2. На основе анализа формирует официальное заявление об области применения системы управления информационной безопасностью. Определяет внутренние и внешние факторы, заинтересованные стороны, их требования и ожидания. Формулирует цели информационной безопасности по критерию SMART, увязывая их с результатами анализа рисков и регуляторными требованиями.
3. Ожидаемый результат: Документ «Границы и область применения системы управления информационной безопасностью», матрица контекста и заинтересованных сторон, перечень целей с показателями достижения, обоснование выбора границ.

Краткое описание и регламент выполнения

1. Изучить теоретический материал и нормативно-правовую базу.
2. Оформить отчет о практической работе в соответствии с требованиями к оформлению практических работ в соответствии с тематикой задания.

Критерии оценки:

Формы текущего контроля	Критерии и нормы оценки
Отчет по практическим работам № 1-8	2 балла – задание выполнено в полном объеме без замечаний - 2 балла – задание не выполнено
Устный опрос	41-62 балла – дан полный, развернутый, аргументированный ответ на 2 вопроса 31-40 баллов – дан неполный ответ на 2 вопроса 21-30 баллов – дан полный, развернутый, аргументированный ответ на 1 вопрос 1-20 баллов – дан неполный ответ на 1 вопрос 0 баллов – не дан ни один ответ на 2 вопроса
Посещаемость	10 баллов - обучающийся посещает все занятия. Для обучающихся с менее чем 100% посещаемостью оценка рассчитывается пропорционально количеству посещенных занятий

7.2.2. Тестирование

Типовой пример тестового задания

Какой метод оценки рисков предполагает расчёт годового ожидаемого ущерба (ALE) по формуле: Ценность актива × Фактор утраты × Частота в год?

Выберите один из 4 вариантов ответа:

- 1) Качественная оценка (матрица 5×5)
- 2) Количественная оценка
- 3) Экспертная оценка
- 4) Анализ «что, если»

Критерии оценки:

Баллы начисляются автоматически пропорционально правильным ответам.

7.3. Оценочные средства для промежуточной аттестации по итогам освоения дисциплины

7.3.1. Вопросы к промежуточной аттестации

Семестр 5

№ п/п	Вопросы к зачету
1.	Раскройте содержание триады базовых свойств информационной безопасности (конфиденциальность, целостность, доступность). Приведите по два практических примера нарушения каждого свойства в прикладной информационной системе предприятия.
2.	Дайте развернутое определение понятия «актив информационной безопасности». Опишите алгоритм идентификации и классификации активов в корпоративной информационной системе на примере системы учёта клиентов.

3.	Объясните различие между понятиями «угроза информационной безопасности», «уязвимость» и «риск». Проиллюстрируйте взаимосвязь этих понятий на конкретном сценарии атаки на веб-приложение.
4.	Охарактеризуйте основные категории субъектов, участвующих в управлении информационной безопасностью организации (владелец информации, пользователь, администратор безопасности, регулятор). Укажите их права, обязанности и зоны ответственности.
5.	Раскройте содержание принципа «разделения обязанностей» в управлении информационной безопасностью. Объясните, как реализация этого принципа снижает риск внутренних нарушений, и приведите пример его применения в системе разграничения доступа.
6.	Дайте определение термину «политика информационной безопасности». Опишите требования к структуре и содержанию этого документа, а также процедуру его утверждения и доведения до сотрудников.
7.	Объясните различие между понятиями «информационная безопасность» и «кибербезопасность» в контексте прикладной информатики. В каких ситуациях эти понятия могут пересекаться, а в каких — различаться?
8.	Опишите жизненный цикл информации в информационной системе. На каких этапах жизненного цикла наиболее критичны меры защиты конфиденциальности, а на каких — целостности? Обоснуйте свой ответ.
9.	Раскройте содержание понятия «модель нарушителя информационной безопасности». Какие характеристики нарушителя необходимо учитывать при проектировании системы защиты прикладной информационной системы?
10.	Объясните, почему управление информационной безопасностью следует рассматривать как непрерывный процесс, а не как разовое мероприятие. Какие факторы обуславливают необходимость постоянного пересмотра мер защиты?
11.	Раскройте назначение и структуру системы менеджмента информационной безопасности. Опишите, как модель «Планируй – Делай – Проверь – Воздействуй» реализуется на практике в организации.
12.	Охарактеризуйте требования международного стандарта 27001 к документации системы менеджмента информационной безопасности. Какие документы являются обязательными, а какие — рекомендуемыми?
13.	Объясните назначение «Заявления о применимости» в системе менеджмента информационной безопасности. Опишите алгоритм его формирования на примере организации, внедряющей защиту персональных данных.
14.	Раскройте содержание процесса «Определение контекста организации» при внедрении системы менеджмента информационной безопасности. Какие внутренние и внешние факторы необходимо учитывать?
15.	Опишите процедуру проведения внутреннего аудита системы менеджмента информационной безопасности. Какие этапы включает аудит, кто участвует в его проведении и как оформляются результаты?
16.	Объясните различие между сертификацией системы менеджмента информационной безопасности и декларированием соответствия. В каких случаях организации целесообразно выбирать тот или иной путь подтверждения соответствия?
17.	Раскройте содержание процесса «Анализ со стороны руководства» в системе менеджмента информационной безопасности. Какие вопросы должны рассматриваться на таком анализе и какие решения могут быть приняты?
18.	Опишите иерархию документов в системе менеджмента информационной безопасности (политики, стандарты, процедуры, инструкции). Приведите примеры документов каждого уровня для прикладной информационной системы.

19.	Объясните, как система менеджмента информационной безопасности интегрируется с другими системами менеджмента организации (качество, охрана труда, экология). Какие преимущества даёт такая интеграция?
20.	Раскройте требования к компетенциям персонала, участвующего в управлении информационной безопасностью. Опишите алгоритм оценки и развития компетенций сотрудников в этой области.
21.	Опишите полный цикл процесса управления рисками информационной безопасности. Раскройте содержание каждого этапа и укажите типичные ошибки, допускаемые на практике.
22.	Раскройте различие между качественными, количественными и полуколичественными методами оценки рисков. В каких ситуациях целесообразно применять каждый из методов? Приведите примеры.
23.	Объясните алгоритм идентификации активов, угроз и уязвимостей при проведении оценки рисков. Какие источники информации и методы сбора данных рекомендуется использовать?
24.	Опишите критерии определения приемлемого уровня риска для организации. Как формируются эти критерии и кто принимает окончательное решение об их утверждении?
25.	Раскройте содержание четырёх стратегий обработки рисков: снижение, передача, избегание, принятие. Приведите по два практических примера применения каждой стратегии в прикладной информационной системе.
26.	Объясните порядок формирования плана обработки рисков. Какие разделы должен содержать этот документ и как обеспечивается контроль его выполнения?
27.	Раскройте понятие «остаточный риск». Почему важно документировать остаточные риски и как они учитываются при принятии управленческих решений?
28.	Опишите методику расчёта приоритета рисков на основе оценки вероятности и ущерба. Как визуализировать результаты оценки для представления руководству организации?
29.	Объясните, как учитывать неопределённость и субъективность экспертных оценок при проведении качественной оценки рисков. Какие приёмы позволяют повысить достоверность результатов?
30.	Раскройте особенности управления рисками в условиях быстро меняющейся технологической среды (облачные сервисы, мобильные устройства, интернет вещей). Какие дополнительные факторы необходимо учитывать?
31.	Опишите алгоритм разработки и внедрения политики информационной безопасности в организации. Какие этапы включают процесс согласования, утверждения и доведения политики до сотрудников?
32.	Раскройте содержание политики разграничения доступа. Какие принципы (минимальные привилегии, разделение обязанностей, необходимость знать) должны быть отражены в этом документе?
33.	Объясните различие между политиками, стандартами, процедурами и инструкциями в системе документации по управлению информационной безопасностью. Приведите примеры документов каждого типа для прикладной информационной системы.
34.	Опишите порядок организации обучения и повышения осведомлённости сотрудников в области информационной безопасности. Какие форматы обучения наиболее эффективны для разных категорий персонала?
35.	Раскройте содержание политики использования электронных средств связи (электронная почта, мессенджеры, социальные сети). Какие ограничения и рекомендации должны быть включены в этот документ?

36.	Объясните, как обеспечить актуальность политик и процедур информационной безопасности в условиях изменений в бизнес-процессах и технологиях. Опишите процедуру периодического пересмотра документации.
37.	Раскройте содержание политики резервного копирования и восстановления данных. Какие параметры (периодичность, типы копий, место хранения, проверка целостности) необходимо регламентировать?
38.	Опишите организационные меры защиты информации при удалённой работе сотрудников. Какие требования должны предъявляться к устройствам, каналам связи и процедурам аутентификации?
39.	Объясните назначение и порядок проведения вводного и периодического инструктажей сотрудников по вопросам информационной безопасности. Как документировать факт проведения инструктажа?
40.	Раскройте содержание политики управления учётными записями и паролями. Какие требования к сложности, сроку действия и хранению паролей являются обоснованными с точки зрения безопасности и удобства использования?
41.	Опишите полный процесс управления инцидентами информационной безопасности. Раскройте содержание каждого этапа: подготовка, обнаружение, анализ, сдерживание, ликвидация, восстановление, извлечение уроков.
42.	Раскройте критерии классификации инцидентов информационной безопасности по степени тяжести. Как определяется приоритет реагирования и кто принимает решение о классификации?
43.	Объясните назначение и структуру регламента реагирования на инциденты информационной безопасности. Какие разделы должны быть включены в этот документ для обеспечения эффективности реагирования?
44.	Опишите порядок создания и функционирования группы реагирования на инциденты информационной безопасности. Какие роли и компетенции должны быть представлены в составе группы?
45.	Раскройте различие между управлением инцидентами информационной безопасности и обеспечением непрерывности бизнеса. Как эти процессы взаимодействуют в практической деятельности организации?
46.	Объясните алгоритм разработки плана обеспечения непрерывности бизнеса для прикладной информационной системы. Какие этапы включает анализ воздействия на бизнес и выбор стратегий восстановления?
47.	Опишите требования к резервному копированию данных в контексте обеспечения непрерывности бизнеса. Как определить целевые показатели времени восстановления и точки восстановления?
48.	Раскройте содержание процедуры постинцидентного анализа. Какие вопросы должны быть рассмотрены в отчёте по результатам анализа и как обеспечивается внедрение корректирующих действий?
49.	Объясните порядок организации тренировок и учений по реагированию на инциденты информационной безопасности. Какие сценарии целесообразно отрабатывать и как оценивать эффективность учений?
50.	Опишите ключевые показатели эффективности процесса управления инцидентами информационной безопасности. Как эти показатели используются для совершенствования процессов защиты?
51.	Раскройте систему нормативных правовых актов Российской Федерации, регулирующих вопросы информационной безопасности. Охарактеризуйте сферу применения Федерального закона «О персональных данных», Федерального закона «Об информации, информационных технологиях и о защите информации», Федерального закона «О безопасности критической информационной инфраструктуры».

52.	Опишите требования к защите персональных данных при их обработке в информационных системах. Какие организационные и технические меры должны быть реализованы оператором персональных данных?
53.	Объясните понятие «комплаенс» в области информационной безопасности. Опишите алгоритм формирования реестра применимых требований и контроля их соблюдения в прикладной информационной системе.
54.	Раскройте содержание процесса внутреннего аудита информационной безопасности. Какие этапы включает планирование, проведение и оформление результатов аудита?
55.	Опишите порядок подготовки организации к проверке регулятора в области информационной безопасности. Какие документы и доказательства соответствия необходимо иметь в готовности?
56.	Объясните различие между аудитом соответствия, аудитом безопасности и аудитом эффективности мер защиты. В каких случаях применяется каждый из видов аудита?
57.	Раскройте требования к документированию процессов управления информационной безопасностью для целей комплаенса. Какие доказательства соблюдения требований могут быть запрошены регулятором?
58.	Опишите взаимодействие организации с уполномоченными органами в области информационной безопасности (Федеральная служба по техническому и экспортному контролю, Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, Центр мониторинга и реагирования на компьютерные атаки). В каких ситуациях такое взаимодействие является обязательным?
59.	Объясните порядок уведомления субъектов персональных данных и регулятора о нарушениях безопасности персональных данных. Какие сроки и форматы уведомления установлены законодательством?
60.	Раскройте особенности управления информационной безопасностью в условиях трансграничной передачи данных. Какие правовые и технические меры необходимо учитывать при проектировании прикладных информационных систем с международным компонентом?

7.3.2. Критерии и нормы оценки

Семестр	Форма проведения промежуточной аттестации	Критерии и нормы оценки	
5	Зачет (по накопительному рейтингу)	«зачтено»	55-100 баллов
		«не зачтено»	0-54 баллов

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Обязательная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Прохорова О. В.	Информационная безопасность и защита информации	учебник	2025	эбс-Лань
2	Сычев Ю. Н.	Основы информационной безопасности	учебное пособие	2025	эбс-ZNANIUM
3	Баранова Е. К.	Информационная безопасность и защита информации	учебное пособие	2026	эбс-ZNANIUM
4	Фаронов, А. Е.	Основы информационной безопасности при работе на компьютере	учебное пособие	2024	эбс-IPRbooks

8.2. Дополнительная литература

№ п/п	Авторы, составители	Заглавие (заголовок)	Тип (учебник, учебное пособие, учебно- методическое пособие, практикум, др.)	Год издания	Количество в научной библиотеке / Наименование ЭБС
1	Шаньгин В. Ф.	Информационная безопасность и защита информации	учебное пособие	2019	эбс-IPRbooks
2	Глинская Е. В.	Информационная безопасность конструкций ЭВМ и систем	учебное пособие	2021	эбс-ZNANIUM
3	Ревнивых А. В.	Информационная безопасность в организациях	учебное пособие	2021	эбс-IPRbooks

8.3. Перечень профессиональных баз данных и информационных справочных систем

1. FREEDOM COLLECTION (Полнотекстовая коллекция электронных журналов Elsevier B.V.) <https://www.sciencedirect.com/> неизвестный
2. Nano Database <http://nano.nature.com/> база данных
3. Springer Materials <http://materials.springer.com/> база данных
4. Springer Nature Protocols and Methods <https://experiments.springernature.com/sources/springer-protocols> база данных
5. zbMath <https://zbmath.org/> база данных
6. Springer Nature (Полнотекстовая коллекция журналов) <https://www.springernature.com/gp/products> неизвестный
7. Springer eBooks (Полнотекстовая коллекция электронных книг издательства Springer Nature) <https://link.springer.com/> неизвестный
8. ORBIT INTELLIGENCE (Патентная база компании QUESTEL) <http://www.orbit.com/> база данных
9. CSD-ENTERPRISE (База данных компании CAMBRIDGE CRYST ALLOGRAPHIC DATA CENTER) <https://www.ccdc.cam.ac.uk/structures/> база данных
10. ELIBRARY.RU (электронная библиотека научных публикаций) <http://elibrary.ru> неизвестный
11. "Гарант" <https://www.garant.ru/> ИСС
12. "КонсультантПлюс" <https://www.consultant.ru/> ИСС
13. "Кодекс" <https://kodeks.ru/> ИСС
14. Техэксперт <https://cntd.ru/> ИСС

8.4. Перечень программного обеспечения

№ п/п	Наименование ПО	Реквизиты договора (дата, номер, срок действия)
1	Windows	Windows (Договор № 690 от 19.05.2015г., срок действия - бессрочно);
2	OfficeStandart	OfficeStandart (Договор № 690 от 19.05.2015г., срок действия - бессрочно; Договор № 727 от 20.07.2016г., срок действия - бессрочно)
3.	Консультант+	Консультант+ (Договор №1522 от 25.12.2015, срок действия - бессрочно)

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

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номера аудиторий)	Перечень основного оборудования
1	Помещение для самостоятельной работы обучающихся Д -409	Стол-парты двухместные, стулья, стол преподавательский-, стул преподавательский, передвижная доска, экран, процессор, проектор, компьютерные столы, компьютеры для

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
		студентов с выходом в сеть интернет, компьютер преподавателя, сетевой шкаф
2	Помещение для самостоятельной работы обучающихся УЛК-105	Стол, стулья, стеллажи (в т.ч. выставочные) с книгами, персональные компьютеры, мобильные рабочие места
3	Аудитория веб-конференций. Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации Э-705	Стол преподавательский, экран телевизионный, роутер, стойка для телевизора, веб. камера, транспарант-перетяжка, ширма, наушники, компьютер с выходом в Интернет.
4	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. Д-402	Стол, стулья, стол преподавательский, стул преподавательский, доска аудиторная (меловая), кафедра напольная, проектор, экран выкатной.
5	Лаборатория "Техносферная безопасность. Здания, сооружения и их устойчивость при пожаре". Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. Институт инженерной и экологической безопасности	Стол, стулья, стол преподавательский., стул преподавательский, стулья ученические, доска аудиторная (меловая), шкаф, стенд для размещения документов по охране труда, пожарной безопасности, стол для манекена, манекен, тонометр механический, торс реанимационный, тренажер для постановки клизмы и в/м инъекций, тренажер сердце-легкие и мозговой реанимации максимум 2-01, носилки санитарные., секундомер

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	Д-403	
6	<p>Лаборатория "Техносферная безопасность. Автоматизированные системы управления и связи. Производственная и пожарная автоматика".</p> <p>Учебная аудитория для проведения занятий семинарского типа.</p> <p>Учебная аудитория для курсового проектирования (выполнения курсовых работ).</p> <p>Учебная аудитория для проведения групповых и индивидуальных консультаций</p> <p>Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации.</p> <p>Д-405</p>	<p>Столы ученические двухместные. стол преподавательский, стул преподавательский, стулья ученические, доска аудиторная (меловая), шкаф, стенд для размещения документов по охране труда, пожарной безопасности, стенд для размещения и хранения лабораторных принадлежностей по дисциплине «Пожарная безопасность», огнетушитель ОУБ-7, песочница мини, противогазы в сумке, учебно-лабораторное оборудование «Автоматическая система пожаротушения», учебно-лабораторное оборудование "Охранно-пожарная сигнализация" стенд «Сигнализация пожарно-охранная сигнализация», стенд «Оросители автоматические системы пожаротушения»</p>
7	<p>Лаборатория "Техносферная безопасность".</p> <p>Учебная аудитория для проведения занятий семинарского типа.</p> <p>Учебная аудитория для курсового проектирования (выполнения курсовых работ).</p> <p>Учебная аудитория для проведения групповых и индивидуальных консультаций</p> <p>Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации.</p> <p>Д-407</p>	<p>Столы ученические двухместные, стол преподавательский, стул преподавательский, стулья ученические, доска аудиторная (меловая), шкаф, стенд для размещения документов по охране труда, пожарной безопасности, экран на треноге Da-Lite Versatol 152x152, проектор №265910 Acer P1, ноутбук №6512 BWL HP Compaq nx 7300 CM-430 -, стенд для размещения нормативных документов по дисциплине «Безопасность грузоподъемных машин и механизмов», стенд к лабораторной работе № 2 «Браковка канатных строп».</p>
8	<p>Лаборатория "Техносферная безопасность".</p> <p>Учебная аудитория для проведения занятий семинарского типа.</p> <p>Учебная аудитория для курсового проектирования (выполнения курсовых работ).</p> <p>Учебная аудитория для проведения групповых и индивидуальных консультаций</p>	<p>Столы ученические двухместные, стол преподавательский, стул преподавательский, стулья ученические, доска аудиторная (меловая), шкаф, тумба на колесиках, стенд "Средства индивидуальной защиты", стенд для размещения документов по охране труда, пожарной безопасности, стенд «Материалы и отходы», магнитные доски на колесиках</p>

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий, мастерских и др. объектов для проведения практических и лабораторных занятий, помещений для самостоятельной работы обучающихся (номер аудитории)	Перечень основного оборудования
	Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. Д-408	
9	Лаборатория "Техносферная безопасность". Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. Д-410	Столы ученические двухместные, стол преподавательский, стул преподавательский., стулья ученические, доска аудиторная (меловая), шкаф, стенд для размещения документов по охране труда, пожарной безопасности, стенд «Низковольтная защитная аппаратура», шкаф распределительный, стойка с изолирующими штангами (6 шт), стенд испытательный (щитовая), огнетушитель -, стенд «Электросхемы», стенд проверки электроинструментов СПЭИ-1, стенд «Виды ламп», стенд «Защитные средства и приспособления», установка лабораторная «Модель электродвигателя», стенд «Низковольтная защитная аппаратура»
10	Учебная аудитория для проведения занятий лекционного типа. Учебная аудитория для проведения занятий семинарского типа. Учебная аудитория для курсового проектирования (выполнения курсовых работ). Учебная аудитория для проведения групповых и индивидуальных консультаций. Учебная аудитория для проведения занятий текущего контроля и промежуточной аттестации. Д-413	Столы ученические двухместные , стол преподавательский, стул преподавательский, стулья ученические, доска аудиторная, кафедра напольная, проектор подвесной, экран (с автоматическим приводом), системный блок .