МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Донской казачий государственный институт пищевых технологий и бизнеса (филиал) федерального государственного бюджетного образовательного учреждения «Московский государственный университет технологий и управления имени К.Г. Разумовского (Первый казачий университет)»

Донской казачий государственный институт пищевых технологий и бизнеса (филиал)

УТВЕРЖДАЮ

И.о. директора ДКГИПТиБ (филиала)

_____ Г.В. Павлятенко

«10» 04 2026 г.

Рабочая программа дисциплины (модуля)

Б1.О.04.10 ОБЩЕПРОФЕССИОНАЛЬНЫЙ МОДУЛЬ Информационная безопасность

Кафедра:	Физика, математика и информационные технологии
Направление подготовки:	15.03.04 Автоматизация технологических процессов и производств
Направленность (профиль):	Проектирование автоматизированных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	заочная
Год набора:	2026
Общая трудоемкость:	216 часов/6 з.е.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00AA7853CEFA35F0837BA866654F3503A6
Владелец: Павлятенко Геннадий Владимирович
Действителен: с 08.12.2025 до 03.03.2027

Ростов-на-Дону, 2026 г.

Программу составил(и):
преподаватель Горбунов В.С.

Рабочая программа дисциплины (модуля)
"Информационная безопасность"
разработана на основании учебного плана, утвержденного ученым советом 26 марта 2026 г. протокол № 9 в соответствии с ФГОС ВО Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств (приказ Минобрнауки России от 09.08.2021 г. № 730),

Руководитель ОПОП
Лазаренко С.В.

Рабочая программа обсуждена на заседании обеспечивающей кафедры
Физика, математика и информационные технологии
Протокол от 10 04 2026 г. № 8
И.о. зав. кафедрой Левчук Валерия Владимировна_____

Рабочая программа согласована на заседании выпускающей кафедры
Пищевые технологии и оборудование
Протокол от 10 04 2026 г. № 8
И.о. зав. кафедрой Павлова Ирина Васильевна _____

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ И ОБЪЕМ С РАСПРЕДЕЛЕНИЕМ ПО СЕМЕСТРАМ

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

6. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

9. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цели:

Цель учебной дисциплины заключается в получении обучающимися теоретических
знаний об основах защиты информации, организационных методах защиты информации, математических методах,
лежащих в основе защиты информации с последующим применением в профессиональной сфере

1.2. Задачи:

1. изложение системы основных концепций и понятий, используемых в современных технологиях защиты информации;
2. описание основных подходов, принятых в сфере информационной безопасности;
3. ознакомление с основными инструментальными средствами защиты информации;
4. приобретение навыков работы с аппаратными средствами защиты информации;
5. формирование навыков самостоятельной работы, организации
исследовательской работы

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ И ОБЪЕМ С РАСПРЕДЕЛЕНИЕМ ПО КУРСАМ

Цикл (раздел) ОП: "Информационная безопасность"

Дисциплина относится к обязательной части ОПОП и обязательна для освоения.

Связь с предшествующими дисциплинами (модулями), практиками

№ п/п	Наименование	Курс	Шифр компетенции
1	Электротехника и электроника	3	ОПК-4.1, ОПК-4.2, ОПК-4.3
2	Основы алгоритмизации и программирования	1	ОПК-14.1, ОПК-14.2, ОПК-14.3
3	Основы информационных технологий	1	УК-1.1, УК-1.2, УК-1.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
4	Пакеты прикладных программ для профессиональной деятельности	1	ОПК-2.1, ОПК-2.2, ОПК-2.3, ОПК-4.1, ОПК-4.2, ОПК-4.3
5	Разработка программных приложений	1	ОПК-14.1, ОПК-14.2, ОПК-14.3

Распределение часов дисциплины

Курс	4		Итого	
Вид занятий	УП	РП		
Лекции	4	4	4	4
Лабораторные	6	6	6	6
Практические	4	4	4	4
В том числе электрон.	14	14	14	14
В том числе в форме практ.подготовки	2		2	
Итого ауд.	14	14	14	14
Контактная работа	14	14	14	14
Сам. работа	189	189	189	189
Часы на контроль	13	13	13	13
Итого	216	216	216	216

Вид промежуточной аттестации:

Экзамен 4 курс

Зачёт 4 курс

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций и индикаторов их

ОПК-14:Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения

ОПК-14.1: Знает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); логику построения и принципы функционирования современных языков программирования и языков работы с базами данных, сред разработки информационных систем и технологий, принципы разработки алгоритмов и компьютерных программ; современные языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий

ОПК-14.2: Умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий; читать коды программных продуктов, написанных на освоенных языках программирования, и вносить требуемые изменения; анализировать профессиональные задачи, разрабатывать подходящие информационные решения; самостоятельно осваивать новые для себя современные языки программирования и языки работы с базами данных, среды, разработки информационных систем и технологий

ОПК-14.3: Владеет навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения; навыками отладки и тестирования прототипов программно-технических комплексов задач

ОПК-4:Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

ОПК-4.1: Знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); современные инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, используемые для решения задач профессиональной деятельности, и принципы их работы

ОПК-4.2: Умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности; анализировать профессиональные задачи, выбирать и использовать подходящие информационные технологии

ОПК-4.3: Владеет навыками работы с данными с помощью информационных технологий; навыками применения современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред, программно-технических платформ и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименования разделов, тем, их краткое содержание и результаты освоения /вид занятия/	Курс	Часы	Интеракт.	Прак. подг.	Индикаторы достижения компетенции	Виды контроля
	Раздел 1.Информационная безопасность						
1.1	**Тема 1. Основные понятия теории информационной безопасности Краткое содержание: История становления теории информационной безопасности. Предметная область теории информационной безопасности. Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Основные принципы построения систем защиты. Концепция комплексной защиты информации. Задачи защиты информации Знать: Историю становления теории информационной безопасности; Предметную область теории информационной безопасности; Основные термины и определения правовых понятий Уметь: анализировать угрозы и риски, связанные с нарушением информационной безопасности, и разрабатывать стратегии и методы их снижения; Применять методы защиты информации; Разрабатывать политики и процедуры безопасности Владеть: Навыками адаптации к изменяющейся угрозной среде; Коммуникационными навыками /Ср/**	4	24	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	вопросы к самоподготовке
1.2	**Тема 2. Информация как объект защиты Краткое содержание:**	4	24	0	0	ОПК-4.1,ОПК-	вопросы к самоподготовке

	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 Знать: Уровни представления информации; Основные свойства защищаемой информации; Виды и формы представления информации; Информационные ресурсы; Структура и шкала ценности информации Уметь: Анализировать и классифицировать информацию; Оценивать ценность информации; Разрабатывать стратегии защиты информации; Применять правовые нормы Владеть: Навыками оценки и классификации информации; Техниками защиты информации; Инструментами анализа информационных ресурсов /Ср/					4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	
1.3	**Тема 3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности Краткое содержание: Информационная безопасность и ее место в системе национальной безопасности Российской Федерации. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность. Знать: Концепцию комплексного обеспечения информационной безопасности, включая основные принципы и подходы; Основные органы обеспечения информационной безопасности и их роли в защите информации; Нормативные акты, регулирующие деятельность в области информационной безопасности Уметь: Оценивать уровень информационной безопасности и выявлять уязвимости в информационных системах; Применять методы защиты информации, включая шифрование, аутентификацию, и контроль доступа; Анализировать риски и разрабатывать стратегии по улучшению информационной безопасности Владеть: Навыками построения и управления информационной безопасностью в организации, включая планирование, внедрение и контроль мер по защите информации;**	4	24	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	вопросы к самоподготовке

	Коммуникационными навыками /Ср/						
1.4	**Тема 4. Угрозы информационной безопасности Краткое содержание: Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы Знать: Классификацию угроз информационной безопасности; Основные направления и методы реализации угроз; Неформальную модель нарушителя, включая типичные мотивации, цели и методы атак; Оценку уязвимости системы и ее компонентов, включая методы и инструменты для проведения анализа уязвимостей Уметь: Анализировать уязвимости системы и ее компонентов, используя различные методы и техники; Идентифицировать и классифицировать угрозы информационной безопасности, опираясь на знания о типичных методах атак и сценариях угроз; Применять методы оценки уязвимости для оценки уровня риска для системы и разработки стратегий по их уменьшению Владеть: Навыками использования инструментов для сканирования уязвимостей и анализа безопасности; Навыками разработки и реализации стратегий по обеспечению безопасности информационных систем, включая использование мер защиты, мониторинга угроз и реагирования на инциденты безопасности; Навыками коммуникации /Ср/**	4	24	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	вопросы к самоподготовке
1.5	**Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности. Краткое содержание: 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 Знать: Определение и основные способы несанкционированного доступа; Методы защиты от несанкционированного доступа;**	4	24	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	вопросы к самоподготовке

	Организационные методы защиты от несанкционированного доступа; Инженерно-технические методы защиты от несанкционированного доступа Уметь: разрабатывать и настраивать системы защиты, предотвращающие утечку информации через технические каналы; реализовывать методы идентификации и аутентификации пользователей Владеть: основными принципами криптографии; методами защиты информации на различных уровнях, включая защиту от утечки данных при их хранении, передаче и обработке /Ср/						
1.6	**Тема 6. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа Краткое содержание: 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 Знать: Основные принципы и методы защиты целостности информации; Технологии и методы защиты при хранении, обработке и транспортировке информации; Виды угроз нарушения целостности информации и их характеристики; Основные подходы к построению систем защиты от угрозы отказа доступа к информации Уметь: Применять различные методы и технологии для защиты целостности информации в различных ситуациях; Анализировать и оценивать угрозы нарушения целостности информации и разрабатывать соответствующие стратегии защиты; Разрабатывать и реализовывать системы защиты от угрозы отказа доступа к информации, учитывая конкретные потребности и особенности организации Владеть: Навыками практического применения различных методов и технологий защиты информации в реальных сценариях; Способностью адаптироваться к быстро меняющейся угрозовой обстановке и вносить соответствующие изменения в системы защиты информации /Ср/**	4	24	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	вопросы к самоподготовке
1.7	**Тема 7. Политика и модели безопасности Краткое содержание:**	4	24	0	0	ОПК-4.1,ОПК-	вопросы к самоподготовке

	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 Знать: Основные принципы и концепции политики безопасности; Субъектно-объектные модели разграничения доступа и их основные характеристики; Аксиомы политики безопасности и их значение; Различные типы парольных систем разграничения доступа Уметь: Проектировать и реализовывать политику безопасности для различных типов информационных систем; Применять субъектно-объектные модели разграничения доступа на практике; Создавать и управлять парольными системами разграничения доступа; Применять модели дискреционного и мандатного доступа в соответствии с требованиями системы Владеть: Навыками анализа потребностей в безопасности информационной системы и разработки соответствующей политики безопасности; Навыками использования специализированных инструментов для управления доступом и аутентификации пользователей; Навыками обучения пользователей правилам безопасного использования информационных ресурсов и соблюдения политики безопасности /Ср/					4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	
1.8	**Тема 8. Информационные войны и информационное противоборство Краткое содержание: Определение и основные виды информационных войн. Информационно-техническая война. Информационно-психологическая война Знать: Определение информационных войн и их основные характеристики; Виды информационных войн; Основные принципы и методы проведения информационных войн; Роль информационных технологий и средств массовой информации в информационных войнах Уметь: Анализировать информационную среду и выявлять признаки информационных войн; Оценивать уровень угрозы информационных**	4	21	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	вопросы к самоподготовке

	войн и разрабатывать стратегии и тактики их противодействия; Использовать информационные технологии и средства массовой информации для защиты от информационных атак и распространения пропаганды Владеть: Навыками создания и поддержания информационной безопасности в рамках персонального и организационного уровней; Навыками управления информационными ресурсами и контентом для достижения стратегических целей в информационном пространстве; /Ср/						
1.9	**Тема 1. Основные понятия теории информационной безопасности Краткое содержание: История становления теории информационной безопасности. Предметная область теории информационной безопасности. Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Основные принципы построения систем защиты. Концепция комплексной защиты информации. Задачи защиты информации Знать: Историю становления теории информационной безопасности; Предметную область теории информационной безопасности; Основные термины и определения правовых понятий Тема 2. Информация как объект защиты Краткое содержание: 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 Знать: Уровни представления информации; Основные свойства защищаемой информации; Виды и формы представления информации; Информационные ресурсы; Структура и шкала ценности информации /Лек/**	4	1	0	0	ОПК-4.1,ОПК-14.1	устный опрос
1.10	**Тема 3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности Краткое содержание: Информационная безопасность и ее место в системе национальной безопасности Российской Федерации. Органы обеспечения**	4	1	0	0	ОПК-4.1,ОПК-14.1	устный опрос

	информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность. Знать: Концепцию комплексного обеспечения информационной безопасности, включая основные принципы и подходы; Основные органы обеспечения информационной безопасности и их роли в защите информации; Нормативные акты, регулирующие деятельность в области информационной безопасности Тема 4. Угрозы информационной безопасности Краткое содержание: Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы Знать: Классификацию угроз информационной безопасности; Основные направления и методы реализации угроз; Неформальную модель нарушителя, включая типичные мотивации, цели и методы атак; Оценку уязвимости системы и ее компонентов, включая методы и инструменты для проведения анализа уязвимостей /Лек/						
1.11	**Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности. Краткое содержание: 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 Знать: Определение и основные способы несанкционированного доступа; Методы защиты от несанкционированного доступа; Организационные методы защиты от несанкционированного доступа; Инженерно-технические методы защиты от несанкционированного доступа Тема 6. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа Краткое содержание: Защита целостности информации при хранении. Защита целостности**	4	1	0	0	ОПК-4.1,ОПК-14.1	устный опрос

	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 Знать: Основные принципы и методы защиты целостности информации; Технологии и методы защиты при хранении, обработке и транспортировке информации; Виды угроз нарушения целостности информации и их характеристики; Основные подходы к построению систем защиты от угрозы отказа доступа к информации /Лек/						
1.12	**Тема 7. Политика и модели безопасности Краткое содержание: 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 Знать: Основные принципы и концепции политики безопасности; Субъектно-объектные модели разграничения доступа и их основные характеристики; Аксиомы политики безопасности и их значение; Различные типы парольных систем разграничения доступа** **Тема 8. Информационные войны и информационное противоборство Краткое содержание: Определение и основные виды информационных войн. Информационно-техническая война. Информационно-психологическая война Знать: Определение информационных войн и их основные характеристики; Виды информационных войн; Основные принципы и методы проведения информационных войн; Роль информационных технологий и средств массовой информации в информационных войнах /Лек/**	4	1	0	0	ОПК-4.1,ОПК-14.1	устный опрос
1.13	**Тема 3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности Краткое содержание: Информационная безопасность и ее место в системе национальной**	4	1	0	0	ОПК-4.2,ОПК-4.3,ОПК-14.2,ОПК-14.3	отчет по практической работе, тестирование

	безопасности Российской Федерации. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность. Уметь: Оценивать уровень информационной безопасности и выявлять уязвимости в информационных системах; Применять методы защиты информации, включая шифрование, аутентификацию, и контроль доступа; Анализировать риски и разрабатывать стратегии по улучшению информационной безопасности Владеть: Навыками построения и управления информационной безопасностью в организации, включая планирование, внедрение и контроль мер по защите информации; Коммуникационными навыками /Пр/						
1.14	**Тема 4. Угрозы информационной безопасности Краткое содержание: Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы Уметь: Анализировать уязвимости системы и ее компонентов, используя различные методы и техники; Идентифицировать и классифицировать угрозы информационной безопасности, опираясь на знания о типичных методах атак и сценариях угроз; Применять методы оценки уязвимости для оценки уровня риска для системы и разработки стратегий по их уменьшению Владеть: Навыками использования инструментов для сканирования уязвимостей и анализа безопасности; Навыками разработки и реализации стратегий по обеспечению безопасности информационных систем, включая использование мер защиты, мониторинга угроз и реагирования на инциденты безопасности; Навыками коммуникации /Пр/**	4	1	0	0	ОПК-4.2,ОПК-4.3,ОПК-14.2,ОПК-14.3	отчет по практической работе, тестирование
1.15	**Тема 7. Политика и модели безопасности Краткое содержание: 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**	4	2	0	0	ОПК-4.2,ОПК-4.3,ОПК-14.2,ОПК-14.3	отчет по практической работе, тестирование

	тематического разграничения доступа. Ролевая модель безопасности Уметь: Проектировать и реализовывать политику безопасности для различных типов информационных систем; Применять субъектно-объектные модели разграничения доступа на практике; Создавать и управлять парольными системами разграничения доступа; Применять модели дискреционного и мандатного доступа в соответствии с требованиями системы Владеть: Навыками анализа потребностей в безопасности информационной системы и разработки соответствующей политики безопасности; Навыками использования специализированных инструментов для управления доступом и аутентификации пользователей; Навыками обучения пользователей правилам безопасного использования информационных ресурсов и соблюдения политики безопасности /Пр/						
1.16	**Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности. Краткое содержание: 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 Уметь: разрабатывать и настраивать системы защиты, предотвращающие утечку информации через технические каналы; реализовывать методы идентификации и аутентификации пользователей Владеть: основными принципами криптографии; методами защиты информации на различных уровнях, включая защиту от утечки данных при их хранении, передаче и обработке /Лаб/**	4	3	0	0	ОПК-4.2,ОПК-4.3,ОПК-14.2,ОПК-14.3	отчет по лабораторной работе
1.17	**Тема 6. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа Краткое содержание: Защита целостности информации при хранении. Защита целостности**	4	3	0	0	ОПК-4.2,ОПК-4.3,ОПК-14.2,ОПК-14.3	отчет по лабораторной работе

	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 Уметь: Применять различные методы и технологии для защиты целостности информации в различных ситуациях; Анализировать и оценивать угрозы нарушения целостности информации и разрабатывать соответствующие стратегии защиты; Разрабатывать и реализовывать системы защиты от угрозы отказа доступа к информации, учитывая конкретные потребности и особенности организации Владеть: Навыками практического применения различных методов и технологий защиты информации в реальных сценариях; Способностью адаптироваться к быстро меняющейся угрозовой обстановке и вносить соответствующие изменения в системы защиты информации /Лаб/						
	Раздел 2.Контроль						
2.1	**Зачет Знать: Историю становления теории информационной безопасности; Предметную область теории информационной безопасности; Основные термины и определения правовых понятий; Уровни представления информации; Основные свойства защищаемой информации; Виды и формы представления информации; Информационные ресурсы; Структура и шкала ценности информации; Концепцию комплексного обеспечения информационной безопасности, включая основные принципы и подходы; Основные органы обеспечения информационной безопасности и их роли в защите информации; Нормативные акты, регулирующие деятельность в области информационной безопасности; Классификацию угроз информационной безопасности; Основные направления и методы реализации угроз; Неформальную модель нарушителя, включая типичные мотивации, цели и методы атак; Оценку уязвимости системы и ее компонентов, включая методы и инструменты для проведения анализа уязвимостей Уметь: анализировать угрозы и риски,**	4	0	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	вопросы к зачету, тестирование

	связанные с нарушением информационной безопасности, и разрабатывать стратегии и методы их снижения; Применять методы защиты информации; Разрабатывать политики и процедуры безопасности; Анализировать и классифицировать информацию; Оценивать ценность информации; Разрабатывать стратегии защиты информации; Применять правовые нормы; Оценивать уровень информационной безопасности и выявлять уязвимости в информационных системах; Применять методы защиты информации, включая шифрование, аутентификацию, и контроль доступа; Анализировать риски и разрабатывать стратегии по улучшению информационной безопасности; Анализировать уязвимости системы и ее компонентов, используя различные методы и техники; Идентифицировать и классифицировать угрозы информационной безопасности, опираясь на знания о типичных методах атак и сценариях угроз; Применять методы оценки уязвимости для оценки уровня риска для системы и разработки стратегий по их уменьшению Владеть: Навыками адаптации к изменяющейся угрозной среде; Коммуникационными навыками; Навыками оценки и классификации информации; Техниками защиты информации; Инструментами анализа информационных ресурсов; Навыками построения и управления информационной безопасностью в организации, включая планирование, внедрение и контроль мер по защите информации; Коммуникационными навыками; Навыками использования инструментов для сканирования уязвимостей и анализа безопасности; Навыками разработки и реализации стратегий по обеспечению безопасности информационных систем, включая использование мер защиты, мониторинга угроз и реагирования на инциденты безопасности; Навыками коммуникации /Зачёт/						
2.2	**Экзамен** **ОПК-4.1 Знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов**	4	13	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	вопросы к экзамену, тестирование

	(информационные технологии); современные инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, используемые для решения задач профессиональной деятельности, и принципы их работы **ОПК-4.2 Умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности; анализировать профессиональные задачи, выбирать и использовать подходящие информационные технологии** **ОПК-4.3 Владеет навыками работы с данными с помощью информационных технологий; навыками применения современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред, программно-технических платформ и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности** **ОПК-14.1 Знает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); логику построения и принципы функционирования современных языков программирования и языков работы с базами данных, сред разработки информационных систем и технологий, принципы разработки алгоритмов и компьютерных программ; современные языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий** **ОПК-14.2 Умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического**						

	применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий; читать коды программных продуктов, написанных на освоенных языках программирования, и вносить требуемые изменения; анализировать профессиональные задачи, разрабатывать подходящие информационные решения; самостоятельно осваивать новые для себя современные языки программирования и языки работы с базами данных, среды, разработки информационных систем и технологий **ОПК-14.3 Владеет навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения; навыками отладки и тестирования прототипов программно-технических комплексов задач /Экзамен/**						

Перечень применяемых активных и интерактивных образовательных технологий:
Информационные технологии

Личностно ориентированная технология, способ организации самостоятельной деятельности учащихся, направленный на решение задачи учебного проекта

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Самостоятельная (внеаудиторная) работа обучающегося (далее - СРС) – это планируемая учебная, практическая, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное время (свободное от аудиторных учебных занятий) по заданию и при методическом руководстве научно-педагогического работника (далее – преподаватель) и (или) лиц, привлекаемых к реализации основных профессиональных образовательных программ на иных условиях, но без их непосредственного участия.
СРС по заданию и при методическом руководстве преподавателя и (или) лиц, привлекаемых к реализации основных профессиональных образовательных программ на иных условиях, реализуется во время групповых консультаций и (или) индивидуальной работы обучающихся с преподавателями Университета и (или) лиц, привлекаемых к реализации образовательных программ на иных условиях (в том числе индивидуальных консультаций), а также во время текущего контроля выполнения заданий, отнесенных к самостоятельной работе обучающихся.
Целью СРС является овладение формирование компетенций через овладение знаниями, умениями и навыками профессиональной деятельности по направлению подготовки (специальности). Самостоятельная работа является обязательной для каждого обучающегося.
Формы самостоятельной работы обучающихся определяются преподавателями кафедр Университета при разработке рабочих программ дисциплин (модулей), рабочих программ практик, программ государственной итоговой (итоговой) аттестации, методических указаний по выполнению практических, лабораторных работ, написанию курсовых работ/проектов и ВКР в соответствии с их содержанием.
В Университете оборудованы специальные помещения для самостоятельной работы обучающихся. Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к информационно -телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета.

6. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

6.1. Перечень компетенций с указанием уровней их сформированности

ОПК-14:Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения

Недостаточный уровень:

Знание процессов, методов поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); логику построения и принципы функционирования современных языков программирования и языков работы с базами данных, сред разработки информационных систем и технологий, принципы разработки алгоритмов и компьютерных программ; современные языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий не

сформировано

Умение выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий; читать коды программных продуктов, написанных на освоенных языках программирования, и вносить требуемые изменения; анализировать профессиональные задачи, разрабатывать подходящие информационные решения; самостоятельно осваивать новые для себя современные языки программирования и языки работы с базами данных, среды, разработки информационных систем и технологий не сформировано

Владение навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения; навыками отладки и тестирования прототипов программно-технических комплексов задач не сформировано

Пороговый уровень:

Знает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии)

Умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач

Владеет навыками разработки оригинальных алгоритмов и компьютерных программ

Продвинутый уровень:

Знает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); логику построения и принципы функционирования современных языков программирования и языков работы с базами данных

Умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий

Владеет навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения

Высокий уровень:

Знает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); логику построения и принципы функционирования современных языков программирования и языков работы с базами данных, сред разработки информационных систем и технологий, принципы разработки алгоритмов и компьютерных программ; современные языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий

Умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий; читать коды программных продуктов, написанных на освоенных языках программирования, и вносить требуемые изменения; анализировать профессиональные задачи, разрабатывать подходящие информационные решения; самостоятельно осваивать новые для себя современные языки программирования и языки работы с базами данных, среды, разработки информационных систем и технологий

Владеет навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения; навыками отладки и тестирования прототипов программно-технических комплексов задач

ОПК-4:Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Недостаточный уровень:

Знание процессов, методов поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); современные инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, используемые для решения задач профессиональной деятельности, и принципы их работы не сформировано

Умение выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности; анализировать профессиональные задачи, выбирать и использовать подходящие информационные технологии не сформировано

Владение навыками работы с данными с помощью информационных технологий; навыками применения современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред, программно-технических платформ и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности не сформировано

Пороговый уровень:

Знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (информационные технологии)

Умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства

Владеет навыками работы с данными с помощью информационных технологий

Продвинутый уровень:

Знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); современные инструментальные среды, программно-технические платформы и программные средства

Умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства

Владеет навыками работы с данными с помощью информационных технологий; навыками применения современных информационно-коммуникационных и интеллектуальных технологий

Высокий уровень:

Знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); современные инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, используемые для решения задач профессиональной деятельности, и принципы их работы

Умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности; анализировать профессиональные задачи, выбирать и использовать подходящие информационные технологии

Владеет навыками работы с данными с помощью информационных технологий; навыками применения современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред, программно-технических платформ и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности

6.2. Описание критериев оценивания успеваемости

НЕДОСТАТОЧНЫЙ УРОВЕНЬ	ПОРОГОВЫЙ УРОВЕНЬ	ПРОДВИНУТЫЙ УРОВЕНЬ	ВЫСОКИЙ УРОВЕНЬ
Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины (модуля); - отсутствие готовности (способности) к дискуссии и низкая степень контактности.	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины (модуля); - умение без грубых ошибок решать практические задания, которые следует выполнить.	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала; - способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины (модуля); - наличие собственной обоснованной позиции по обсуждаемым вопросам; - незначительные оговорки и неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.

Оценка «незачет», «неудовлетворительно»	Оценка «зачтено/удовлетворительно», «удовлетворительно»	Оценка «зачтено/хорошо», «хорошо»	Оценка «зачтено/отлично», «отлично»

6.3. Оценочные средства текущего контроля

ВОПРОСЫ К УСТНОМУ ОПРОСУ

Тема 1. Основные понятия теории информационной безопасности

1. Что такое информационная безопасность?
2. Каковы основные составляющие информационной безопасности?
3. Что такое конфиденциальность информации?
4. Что такое целостность информации?
5. Что такое доступность информации?
6. Какие существуют основные виды угроз информационной безопасности?
7. Что такое риск информационной безопасности?
8. Что такое уязвимость информационной системы?
9. Что такое политика безопасности?
10. Какие существуют основные принципы обеспечения информационной безопасности?

Тема 2. Информация как объект защиты

1. Что такое информация с точки зрения информационной безопасности?
2. Какие существуют категории информации?
3. Что такое конфиденциальная информация?
4. Что такое коммерческая тайна?
5. Что такое государственная тайна?
6. Какие существуют виды информационных ресурсов?
7. Что такое информационная система?
8. Что такое информационно-телекоммуникационная сеть?
9. Каковы основные требования к защите информации?
10. Какие существуют методы и средства защиты информации?

Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности

1. Что такое конфиденциальность информации?
2. Какие существуют угрозы нарушения конфиденциальности информации?
3. Что такое криптография и какова ее роль в обеспечении конфиденциальности?
4. Какие существуют виды криптографических алгоритмов?
5. Что такое симметричное шифрование?
6. Что такое асимметричное шифрование?
7. Что такое электронная цифровая подпись?
8. Что такое управление доступом и его роль в обеспечении конфиденциальности?
9. Какие существуют модели управления доступом?
10. Какие существуют технические и организационные меры защиты конфиденциальности информации?

Тема 6. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа

1. Что такое целостность информации?
2. Какие существуют угрозы нарушения целостности информации?
3. Что такое контроль целостности и его роль в обеспечении целостности информации?
4. Какие существуют методы контроля целостности?
5. Что такое электронная цифровая подпись и ее роль в обеспечении целостности?
6. Что такое резервное копирование и его роль в обеспечении целостности информации?
7. Что такое отказ в обслуживании и его последствия?
8. Какие существуют виды атак, приводящих к отказу в обслуживании?
9. Что такое резервирование и его роль в обеспечении доступности информации?
10. Какие существуют технические и организационные меры защиты от угрозы нарушения целостности и отказа доступа?

ВОПРОСЫ К САМОПОДГОТОВКЕ

Тема 1. Основные понятия теории информационной безопасности

1. Какова предметная область теории информационной безопасности?
2. Каковы основные принципы построения систем защиты информации?
3. Что такое концепция комплексной защиты информации?
4. Каковы основные задачи защиты информации?
5. Как развивалась история становления теории информационной безопасности?
6. Что включают в себя основные термины и определения в области информационной безопасности?
7. Какие методы можно использовать для анализа угроз и рисков информационной безопасности?
8. Как разрабатывать стратегии и методы снижения угроз информационной безопасности?
9. Какие навыки необходимы для адаптации к изменяющейся угрозной среде?
10. Почему важны коммуникационные навыки в области информационной безопасности?

Тема 2. Информация как объект защиты

1. Что такое уровни представления информации?
2. Каковы основные свойства защищаемой информации?
3. Какие существуют виды и формы представления информации?
4. Что такое информационные ресурсы?

5. Как определяется структура и шкала ценности информации?
6. На какие категории можно классифицировать информационные ресурсы?
7. Какие правовые режимы существуют для информационных ресурсов?
8. Как можно анализировать и классифицировать информацию?
9. Какие методы используются для оценки ценности информации?
10. Какие техники и инструменты применяются для защиты информации?
Тема 3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности
1. Какое место занимает информационная безопасность в системе национальной безопасности Российской Федерации?
2. Какие органы обеспечивают информационную безопасность и защиту информации в России?
3. Каковы функции и задачи органов обеспечения информационной безопасности?
4. Какова нормативная деятельность органов обеспечения информационной безопасности?
5. Что такое концепция комплексного обеспечения информационной безопасности?
6. Каковы основные принципы и подходы концепции комплексного обеспечения информационной безопасности?
7. Как можно оценить уровень информационной безопасности и выявить уязвимости в информационных системах?
8. Какие методы защиты информации используются в рамках концепции комплексного обеспечения информационной безопасности?
9. Как анализируются риски и разрабатываются стратегии по улучшению информационной безопасности?
10. Какие навыки необходимы для построения и управления информационной безопасностью в организации?
Тема 4. Угрозы информационной безопасности
1. Что такое анализ уязвимостей системы?
2. Как классифицируются угрозы информационной безопасности?
3. Каковы основные направления и методы реализации угроз информационной безопасности?
4. Что такое неформальная модель нарушителя?
5. Как проводится оценка уязвимости системы?
6. Какие существуют методы анализа уязвимостей системы и ее компонентов?
7. Как можно идентифицировать и классифицировать угрозы информационной безопасности?
8. Какие методы используются для оценки уязвимости и уровня риска для системы?
9. Какие инструменты применяются для сканирования уязвимостей и анализа безопасности?
10. Как разрабатываются и реализуются стратегии по обеспечению безопасности информационных систем?
Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности
1. Что такое несанкционированный доступ и каковы его основные способы?
2. Какие существуют методы защиты от несанкционированного доступа?
3. Какие организационные методы используются для защиты от несанкционированного доступа?
4. Какие инженерно-технические методы применяются для защиты от несанкционированного доступа?
5. Как построить системы защиты от угрозы утечки информации по техническим каналам?
6. Что такое идентификация и аутентификация, и как они реализуются в системах защиты?
7. Каковы основные направления и цели использования криптографических методов?
8. Как защитить конфиденциальность информации на уровне ее содержания?
9. Какие существуют технологии и средства защиты информации от несанкционированного доступа?
10. Как обеспечить защиту конфиденциальности при хранении, передаче и обработке информации?
Тема 6. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа
1. Как обеспечить защиту целостности информации при ее хранении?
2. Какие методы используются для защиты целостности информации при ее обработке?
3. Как защитить целостность информации при ее транспортировке?
4. Что такое защита целостности информации на уровне ее содержания?
5. Каковы основные подходы к построению систем защиты от угрозы отказа доступа к информации?
6. Что такое защита семантического анализа и актуальности информации?
7. Какие виды угроз нарушения целостности информации существуют?
8. Как анализировать и оценивать угрозы нарушения целостности информации?
9. Какие технологии и методы применяются для защиты от угрозы отказа доступа к информации?
10. Как адаптировать системы защиты информации к изменяющейся угрозной обстановке?
Тема 7. Политика и модели безопасности
1. Что такое политика безопасности и каковы ее основные принципы?
2. Что такое субъектно-объектные модели разграничения доступа?
3. Каковы аксиомы политики безопасности и их значение?
4. Что такое политика и модели дискреционного доступа?
5. Какие существуют парольные системы разграничения доступа?
6. Что такое политика и модели мандатного доступа?
7. Что такое теоретико-информационные модели безопасности?
8. Что такое политика и модели тематического разграничения доступа?
9. Что такое ролевая модель безопасности?
10. Как проектировать и реализовывать политику безопасности
Тема 8. Информационные войны и информационное противоборство
1. Что такое информационная война и каковы ее основные виды?
2. Что понимается под информационно-технической войной?
3. Что такое информационно-психологическая война?
4. Каковы основные принципы и методы ведения информационных войн?
5. Какова роль информационных технологий в информационных войнах?
6. Как средства массовой информации используются в информационных войнах?
7. Как проанализировать информационную среду на предмет признаков информационной войны?

8. Какие стратегии и тактики можно использовать для противодействия информационным войнам?
9. Как создать и поддерживать информационную безопасность на персональном и организационном уровнях?
10. Какие навыки управления информационными ресурсами и контентом необходимы для достижения целей в информационном пространстве?

ТЕКУЩЕЕ ТЕСТИРОВАНИЕ
Тема 1. Основные понятия теории информационной безопасности
1. Что не относится к основным принципам обеспечения информационной безопасности? а) Конфиденциальность б) Целостность в) Доступность г) Скорость передачи данных
2. Какой компонент не входит в концепцию комплексной защиты информации? а) Правовое обеспечение б) Организационное обеспечение в) Инженерно-техническое обеспечение г) Коммерческое обеспечение
3. Что является предметной областью теории информационной безопасности? а) Разработка программного обеспечения б) Защита информации и инфраструктуры в) Создание аппаратного обеспечения г) Обслуживание компьютерных сетей
4. Какой навык не требуется для адаптации к изменяющейся угрозной среде? а) Аналитические способности б) Гибкость в) Знание языков программирования г) Способность к обучению
5. Что не относится к основным задачам защиты информации? а) Конфиденциальность б) Целостность в) Доступность г) Совместимость
6. На что направлены коммуникационные навыки в сфере информационной безопасности? а) Обмен информацией и координация действий б) Написание программного кода в) Конфигурирование сетевого оборудования г) Управление персоналом
7. Какой термин определяет защиту информации от несанкционированного доступа? а) Целостность б) Конфиденциальность в) Доступность г) Аутентичность
8. Что такое риск в контексте информационной безопасности? а) Вероятность нарушения целостности данных б) Несанкционированный доступ к информации в) Вероятность реализации угрозы и ее последствия г) Нарушение политики безопасности
9. Какой метод используется для анализа рисков информационной безопасности? а) Метод контрольных сумм б) Криптографическое шифрование в) Анализ уязвимостей г) Разграничение доступа
10. Что такое политика безопасности? а) Техническая документация б) Совокупность правил обработки информации в) Инструкция по эксплуатации оборудования г) Методика тестирования на проникновение

Тема 2. Информация как объект защиты
1. Что не относится к основным свойствам защищаемой информации? а) Конфиденциальность б) Целостность в) Доступность г) Юридическая сила
2. На какие уровни делится представление информации? а) Данные, знания, процедуры б) Открытая, конфиденциальная, секретная в) Текстовая, числовая, графическая
г) Структурированная, неструктурированная
3. Какой критерий не используется для определения ценности информации? а) Важность б) Срок действия в) Секретность г) Стоимость
4. Что не относится к информационным ресурсам? а) Данные б) Программы в) Информационные технологии г) Денежные средства
5. Как классифицируется информация по степени секретности? а) Общедоступная, ограниченного доступа, совершенно секретная б) Открытая, конфиденциальная, секретная в) Публичная, частная, государственная тайна г) Несекретная, коммерческая тайна, государственная тайна
6. Какой метод не используется для оценки ценности информации? а) Оценка рисков б) Экспертные методы в) Метод контрольных сумм г) Бальная оценка
7. Что не относится к видам представления информации? а) Текстовая б) Числовая в) Графическая г) Коммерческая
8. Какой инструмент применяется для анализа информационных ресурсов? а) Межсетевой экран б) Антивирусное ПО в) Средство протоколирования и аудита г) Система обнаружения вторжений
9. Какие правовые нормы регулируют режим информационных ресурсов? а) Законы об информации б) Указы Президента в) Отраслевые стандарты г) Все перечисленное
10. Что входит в понятие информационных ресурсов? а) Только компьютерные системы б) Только данные в) Данные, программы, технологии г) Только информационные системы

Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности
1. Какая технология используется для защиты конфиденциальности данных при передаче по незащищенным каналам связи? а) Шифрование б) Резервное копирование в) Контроль целостности г) Антивирусное программное обеспечение
2. Что из перечисленного не является мерой защиты от угрозы нарушения конфиденциальности? а) Использование брандмауэров б) Применение политик управления доступом в) Шифрование данных г) Создание резервных копий данных
3. Какая технология позволяет обеспечить конфиденциальность данных на уровне хранения? а) Шифрование дисков б) Контроль целостности в) Использование антивирусного программного обеспечения г) Применение брандмауэров
4. Что из перечисленного не относится к мерам защиты от угрозы нарушения конфиденциальности на физическом уровне? а) Использование замков и запорных устройств б) Ограничение физического доступа в помещения в) Применение системы видеонаблюдения г) Использование антивирусного программного обеспечения
5. Какая технология используется для защиты конфиденциальности данных при передаче по защищенным каналам связи? а) Шифрование б) Контроль целостности в) Использование виртуальных частных сетей (VPN) г) Антивирусное программное обеспечение
6. Что из перечисленного не относится к мерам защиты от угрозы нарушения конфиденциальности на программном уровне? а) Использование политик управления доступом б) Применение систем обнаружения вторжений (IDS/IPS) в) Шифрование данных г) Контроль целостности данных

• Выявите уязвимости и потенциальные угрозы информационной безопасности.
• Разработайте план мероприятий по улучшению информационной безопасности, который должен включать:
o Цели и задачи мероприятий.
o Перечень необходимых мер защиты информации.
o Сроки реализации мероприятий.
o Ответственных за выполнение мероприятий.

Тема 4. Угрозы информационной безопасности
1. Анализ уязвимостей системы:
• Выберите для анализа информационную систему, доступ к которой вам предоставлен (например, ваш персональный компьютер, веб-сайт, сервер).
• Используя различные методы и инструменты (сканеры уязвимостей, системы оценки безопасности, анализ кода), проведите анализ уязвимостей выбранной системы.
• Зафиксируйте все найденные уязвимости, описав их тип, описание, уровень опасности и возможные последствия эксплуатации.
2. Классификация угроз:
• Определите, какие угрозы информационной безопасности могут быть реализованы с помощью найденных уязвимостей.
• Сгруппируйте угрозы по категориям (например, по типу воздействия, по типу источника угрозы, по типу цели атаки).
• Для каждой группы угроз опишите возможные сценарии их реализации.
3. Оценка уязвимости:
• Проведите количественную или качественную оценку уязвимости системы.
• При количественной оценке используйте методы, основанные на метриках (например, CVSS).
• При качественной оценке используйте экспертные методы.
• Определите уровень риска для системы и ее компонентов.
4. План действий:
• Разработайте план действий по устранению выявленных уязвимостей.
• План должен включать:
o Перечень уязвимостей, которые необходимо устранить.
o Приоритетность устранения уязвимостей.
o Сроки устранения уязвимостей.
o Ответственных за устранение уязвимостей.
o Ресурсы, необходимые для устранения уязвимостей.
o Меры контроля, которые необходимо реализовать после устранения уязвимостей.

Тема 7. Политика и модели безопасности
1. Политика безопасности:
• Ознакомьтесь с основными понятиями политики безопасности: субъекты доступа, объекты доступа, права доступа, дискреционные и мандатные модели доступа.
• Изучите основные принципы политики безопасности: полнота, непротиворечивость, непротиворечивость, минимизация прав доступа.
• Проанализируйте примеры политик безопасности для различных типов информационных систем.
2. Субъектно-объектные модели разграничения доступа:
• Изучите основные типы субъектно-объектных моделей разграничения доступа: матричная модель, списочная модель, модель доступа по ролям.
• Сравните преимущества и недостатки различных моделей.
• Приведите примеры реализации субъектно-объектных моделей разграничения доступа в операционных системах.
3. Парольные системы разграничения доступа:
• Ознакомьтесь с принципами работы парольных систем разграничения доступа.
• Изучите требования к надежным паролям.
• Рассмотрите различные методы аутентификации пользователей: однофакторная аутентификация, двухфакторная аутентификация, многофакторная аутентификация.
• Проанализируйте примеры реализации парольных систем разграничения доступа.
4. Модели дискреционного и мандатного доступа:
• Изучите основные принципы работы моделей дискреционного и мандатного доступа.
• Сравните модели дискреционного и мандатного доступа.
• Приведите примеры реализации моделей дискреционного и мандатного доступа в операционных системах.
5. Теоретико-информационные модели:
• Ознакомьтесь с основными понятиями теоретико-информационных моделей безопасности: информационные потоки, каналы связи, утечка информации, стойкость к утечке информации.
• Изучите методы оценки стойкости информационных систем к утечке информации.
• Приведите примеры использования теоретико-информационных моделей безопасности для проектирования защищенных систем.
6. Модели тематического разграничения доступа:
• Изучите основные принципы работы моделей тематического разграничения доступа.
• Рассмотрите различные типы моделей тематического разграничения доступа: модели на основе меток конфиденциальности, модели на основе ролей, модели на основе контекста.
• Приведите примеры реализации моделей тематического разграничения доступа в информационных системах.
7. Ролевая модель безопасности:
• Ознакомьтесь с основными принципами работы ролевой модели безопасности.

1. Теоретическая часть:
o Изучить лекционные материалы по теме "Защита информации от НСД и утечки по техническим каналам".
o Ознакомиться с основными способами НСД: перехват информации по техническим каналам, использование вредоносных программ, социальная инженерия.
o Изучить организационные методы защиты от НСД: разграничение доступа к информации, обучение персонала, контроль за информационными системами.
o Ознакомиться с инженерно-техническими методами защиты от НСД: защита физических каналов связи, использование средств криптографии, применение систем обнаружения вторжений.
o Изучить методы идентификации и аутентификации пользователей: парольная аутентификация, биометрическая аутентификация, двухфакторная аутентификация.
o Освоить основы криптографии: симметричное шифрование, асимметричное шифрование, электронная цифровая подпись.
o Изучить методы защиты информации на различных уровнях: защита информации при хранении, передаче и обработке.
2. Практическая часть:
o Вариант 1:
 Разработать план мероприятий по защите информации от НСД для конкретной организации.
 Выбрать и обосновать методы защиты от НСД, которые будут использоваться в данной организации.
 Составить спецификацию на необходимые средства защиты информации.
o Вариант 2:
 Настроить систему защиты от утечки информации по техническим каналам на базе программного обеспечения.
 Провести тестирование системы защиты от утечки информации.
 Оценить эффективность работы системы защиты от утечки информации.
o Вариант 3:
 Разработать систему идентификации и аутентификации пользователей для информационной системы.
 Выбрать и обосновать методы идентификации и аутентификации, которые будут использоваться в данной системе.
 Реализовать систему идентификации и аутентификации пользователей.
o Вариант 4:
 Зашифровать конфиденциальную информацию с помощью симметричного алгоритма шифрования.
 Расшифровать зашифрованную информацию.
 Оценить стойкость используемого алгоритма шифрования.
o Вариант 5:
 Создать электронную цифровую подпись (ЭЦП) под электронным документом.
 Проверить подлинность ЭЦП.
 Оценить криптографическую стойкость ЭЦП.
Отчет:
• Описать изученные методы защиты информации от НСД и утечки по техническим каналам.
• Изложить план мероприятий по защите информации от НСД для конкретной организации (вариант 1).
• Описать процесс настройки системы защиты от утечки информации по техническим каналам (вариант 2).
• Привести результаты тестирования системы защиты от утечки информации (вариант 2).
• Описать разработанную систему идентификации и аутентификации пользователей (вариант 3).
• Привести примеры шифрования и расшифрования информации (вариант 4).
• Описать процесс создания и проверки ЭЦП (вариант 5).
• Сделать выводы о результатах работы.

Тема 6. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа
• Теоретическая часть:
• Изучить основные принципы и методы защиты целостности информации.
• Ознакомиться с технологиями и методами защиты при хранении, обработке и транспортировке информации.
• Изучить виды угроз нарушения целостности информации и их характеристики.
• Рассмотреть основные подходы к построению систем защиты от угрозы отказа доступа к информации.
• Практическая часть:
• Вариант 1:
o Разработать модель системы защиты информации от несанкционированного доступа для локальной сети предприятия.
o Выбрать необходимые методы и технологии защиты, обосновав их выбор.
o Описать архитектуру системы защиты информации, включая используемые компоненты и их взаимодействие.
• Вариант 2:
o Разработать модель системы защиты информации от нарушения целостности для базы данных.
o Выбрать необходимые методы и технологии защиты, обосновав их выбор.
o Описать меры и процедуры, направленные на обеспечение целостности информации в базе данных.
• Вариант 3:
o Провести анализ уязвимости информационной системы предприятия.
o Выявить потенциальные угрозы нарушения целостности информации и отказа доступа.

6.4. Оценочные средства промежуточной аттестации
ВОПРОСЫ К ЗАЧЕТУ

ОПК-4

Индикатор достижения компетенции "Знать"
Вопросы на установление последовательности
1. Установите верную последовательность этапов разработки системы защиты данных:
A. Тестирование системы на уязвимости
B. Определение требований к безопасности
C. Внедрение защитных механизмов
D. Проектирование архитектуры системы
2. Установите верную последовательность уровней обработки информации в системах безопасности:
A. Интерпретация данных
B. Сбор данных
C. Анализ данных
D. Хранение данных
3. Установите верную последовательность действий при реагировании на киберинцидент:
A. Устранение последствий
B. Выявление источника угрозы
C. Изоляция пострадавшей системы
D. Оценка ущерба
4. Установите верную последовательность шагов создания политики управления доступом:
A. Определение ролей пользователей
B. Установка правил доступа
C. Мониторинг соблюдения политики
D. Аудит существующих прав доступа
5. Установите верную последовательность этапов оценки рисков информационной безопасности:
A. Идентификация активов
B. Разработка плана управления рисками
C. Оценка вероятности угроз
D. Анализ последствий реализации угроз

Вопросы на установление соответствия
1. Установите соответствие между этапами разработки системы защиты и их характеристиками:
1. Определение требований
2. Проектирование системы
3. Тестирование
4. Внедрение
A. Проверка эффективности защиты
B. Установка программного обеспечения
C. Выбор методов шифрования
D. Составление списка угроз
2. Установите соответствие между уровнями защиты информации и их функциями:
1. Аппаратный уровень
2. Программный уровень
3. Сетевой уровень
4. Пользовательский уровень
A. Контроль доступа через интерфейс
B. Защита передачи данных
C. Обеспечение работы устройств
D. Обнаружение вредоносных программ
3. Установите соответствие между этапами реагирования на инцидент и их задачами:
1. Изоляция
2. Анализ
3. Устранение
4. Восстановление
A. Возвращение системы в рабочее состояние
B. Прекращение распространения угрозы
C. Удаление вредоносного кода
D. Определение причины инцидента
4. Установите соответствие между типами киберугроз и их последствиями:
1. DDoS-атака
2. Кража учетных данных
3. Шифровальщик
4. Подмена данных
A. Потеря доверия к информации
B. Остановка работы системы
C. Утрата доступа к файлам
D. Несанкционированный доступ
5. Установите соответствие между методами защиты и их целями:
1. Резервное копирование
2. Файрвол
3. Антивирус

4. Обучение сотрудников
A. Предотвращение заражения системы
B. Снижение влияния человеческого фактора
C. Восстановление данных после сбоя
D. Фильтрация сетевого трафика

Индикатор достижения компетенции Уметь
1. Выберите правильный ответ и обоснуйте свой выбор. Какой этап является первым при создании системы защиты данных?
A. Внедрение защитных мер
B. Тестирование системы
C. Определение требований к безопасности
D. Мониторинг угроз
2. Выберите правильный ответ и обоснуйте свой выбор. Какой уровень защиты отвечает за безопасность передачи данных?
A. Аппаратный уровень
B. Сетевой уровень
C. Программный уровень
D. Пользовательский уровень
3. Выберите правильный ответ и обоснуйте свой выбор. Какова главная цель политики управления доступом?
A. Увеличение скорости работы системы
B. Обеспечение доступа только авторизованным пользователям
C. Снижение затрат на оборудование
D. Упрощение интерфейса
4. Выберите правильный ответ и обоснуйте свой выбор. Какая угроза приводит к полной остановке работы системы?
A. Кража данных
B. Шифровальщик
C. DDoS-атака
D. Фишинг
5. Выберите правильный ответ и обоснуйте свой выбор. Какой метод защиты помогает восстановить данные после инцидента?
A. Файрвол
B. Резервное копирование
C. Антивирус
D. Контроль доступа
6. Выберите правильный ответ и обоснуйте свой выбор. Что входит в область анализа рисков информационной безопасности?
A. Разработка интерфейса системы
B. Оценка вероятности угроз
C. Создание рекламных материалов
D. Обучение программированию
7. Выберите правильный ответ и обоснуйте свой выбор. Какое свойство информации связано с ее точностью?
A. Доступность
B. Целостность
C. Конфиденциальность
D. Актуальность
8. Выберите правильный ответ и обоснуйте свой выбор. Кто отвечает за тестирование системы защиты перед ее запуском?
A. Пользователи
B. Разработчики
C. Регулирующие органы
D. Маркетологи
9. Выберите правильный ответ и обоснуйте свой выбор. Какой шаг является первым при реагировании на киберинцидент?
A. Восстановление системы
B. Изоляция пострадавшей системы
C. Устранение угрозы
D. Анализ последствий
10. Выберите правильный ответ и обоснуйте свой выбор. Какой принцип защиты предполагает регулярную проверку системы?
A. Многоуровневая защита
B. Постоянный мониторинг
C. Определение активов
D. Шифрование данных

Индикатор достижения компетенции Владеть
1. Прочитайте текст и дайте развернутый ответ: Компания разрабатывает мобильное приложение для управления финансами клиентов, которое будет хранить их банковские данные и историю транзакций. Приложение должно быть защищено от атак и соответствовать стандартам безопасности. Угрозы включают перехват данных и фишинг. Как разработчики могут внедрить принципы безопасности на этапе проектирования, чтобы обеспечить защиту данных и

ОПК-14
Индикатор достижения компетенции Знать:
Вопросы на установление последовательности
1. Установите верную последовательность этапов создания системы обнаружения вторжений:
A. Настройка системы мониторинга
B. Анализ возможных угроз
C. Тестирование реакции на инциденты
D. Определение критических объектов
2. Установите верную последовательность шагов управления инцидентами кибербезопасности:
A. Восстановление нормальной работы системы
B. Идентификация инцидента
C. Уведомление ответственных лиц
D. Анализ причин инцидента
3. Установите верную последовательность этапов разработки политики управления паролями:
A. Определение требований к паролям
B. Внедрение системы проверки паролей
C. Обучение сотрудников правилам
D. Оценка текущих практик
4. Установите верную последовательность действий при внедрении системы шифрования данных:
A. Тестирование алгоритмов шифрования
B. Выбор подходящего алгоритма
C. Интеграция с информационной системой
D. Анализ потребностей в защите
5. Установите верную последовательность этапов обеспечения непрерывности бизнеса:
A. Разработка плана восстановления
B. Оценка критических процессов
C. Реализация защитных мер
D. Тестирование плана

Вопросы на установление соответствия
1. Установите соответствие между этапами управления киберрисками и их характеристиками:
1. Идентификация рисков
2. Оценка рисков
3. Реализация мер
4. Мониторинг рисков
A. Постоянное наблюдение за угрозами
B. Внедрение защитных технологий
C. Выявление потенциальных уязвимостей
D. Определение вероятности и последствий
2. Установите соответствие между уровнями защиты информации и их описаниями:
1. Уровень приложений
2. Уровень сети
3. Уровень устройств
4. Уровень данных
A. Защита от перехвата трафика
B. Шифрование хранимой информации
C. Контроль доступа к программам
D. Обновление прошивок оборудования
3. Установите соответствие между типами кибератак и их характеристиками:
1. SQL-инъекция
2. Социальная инженерия
3. Атака "человек посередине"
4. Ransomware
A. Манипуляция пользователями
B. Шифрование данных с выкупом
C. Внедрение кода в базу данных
D. Перехват коммуникаций
4. Установите соответствие между методами защиты и их задачами:
1. Брандмауэр
2. Антивирус
3. Резервное копирование
4. Двухфакторная аутентификация
A. Защита от вредоносного ПО
B. Подтверждение личности пользователя
C. Фильтрация сетевого трафика
D. Восстановление данных

5. Установите соответствие между принципами кибербезопасности и их описаниями:
1. Конфиденциальность
2. Целостность
3. Доступность
4. Аутентичность
A. Данные неизменны и достоверны
B. Данные доступны авторизованным пользователям
C. Данные защищены от утечек
D. Подтверждение подлинности источника

Индикатор достижения компетенции Уметь
1. Выберите правильный ответ. Какой этап является первым при создании системы обнаружения вторжений?
A. Настройка системы мониторинга
B. Анализ возможных угроз
C. Тестирование реакции на инциденты
D. Определение критических объектов
2. Выберите правильный ответ. Какой уровень защиты отвечает за шифрование хранимой информации?
A. Уровень приложений
B. Уровень сети
C. Уровень устройств
D. Уровень данных
3. Выберите правильный ответ. Какова основная цель управления киберрисками?
A. Разработка новых алгоритмов
B. Снижение последствий угроз
C. Обучение пользователей
D. Создание резервных копий
4. Выберите правильный ответ. Какая атака связана с манипуляцией пользователями?
A. SQL-инъекция
B. Социальная инженерия
C. Атака "человек посередине"
D. Ransomware
5. Выберите правильный ответ. Какой метод защиты фильтрует сетевой трафик?
A. Брандмауэр
B. Антивирус
C. Резервное копирование
D. Двухфакторная аутентификация
6. Выберите правильный ответ. Что относится к задачам кибербезопасности?
A. Анализ сетевых атак
B. Разработка веб-сайтов
C. Управление складом
D. Маркетинговые исследования
7. Выберите правильный ответ. Какое свойство информации связано с ее доступностью авторизованным пользователям?
A. Конфиденциальность
B. Целостность
C. Доступность
D. Аутентичность
8. Выберите правильный ответ. Кто отвечает за разработку политики управления паролями в компании?
A. Сотрудники техподдержки
B. Руководство компании
C. Внешние аудиторы
D. Поставщики ПО
9. Выберите правильный ответ. Какой шаг является первым при управлении инцидентами?
A. Восстановление системы
B. Идентификация инцидента
C. Уведомление ответственных лиц
D. Анализ причин инцидента
10. Выберите правильный ответ. Какой принцип защиты предполагает подтверждение подлинности источника?
A. Конфиденциальность
B. Целостность
C. Доступность
D. Аутентичность

Индикатор достижения компетенции Владеть
1. Прочитайте текст и дайте развернутый ответ: Компания разрабатывает приложение для управления финансами клиентов, которое будет хранить конфиденциальные данные. Приложение должно быть защищено от атак и соответствовать стандартам. Как внедрить меры кибербезопасности на этапе разработки?
2. Прочитайте текст и дайте развернутый ответ: Организация обнаружила несанкционированный доступ к своей сети, что угрожает конфиденциальности данных. Необходимо минимизировать ущерб. Как разработать план реагирования на инцидент?
3. Прочитайте текст и дайте развернутый ответ: Компания собирает данные о клиентах для аналитики, включая

7. Прочитайте текст и дайте развернутый ответ: Системный администратор заметил аномалии в сетевом трафике, что может указывать на атаку. Как провести анализ и устранить угрозу?
8. Прочитайте текст и дайте развернутый ответ: Компания получила угрозу кибератаки, которая может нарушить работу серверов. Как оценить угрозу и подготовиться к последствиям?
9. Прочитайте текст и дайте развернутый ответ: Компания запускает платформу для онлайн-курсов, где будут храниться данные пользователей. Какие угрозы учитывать и какие меры защиты внедрить?
10. Прочитайте текст и дайте развернутый ответ: Сотрудник сообщил о компрометации учетной записи, что угрожает безопасности данных. Как расследовать инцидент и предотвратить повторение?

ВОПРОСЫ К ЭКЗАМЕНУ:

ОПК-4
Индикатор достижения компетенции Знать:
Вопросы на установление последовательности
1. Установите верную последовательность этапов разработки системы защиты от несанкционированного доступа (НСД):
A. Настройка средств аутентификации
B. Анализ уязвимостей системы
C. Внедрение криптографических методов
D. Определение объектов защиты
2. Установите верную последовательность действий при реализации организационных мер защиты от НСД:
A. Обучение сотрудников
B. Разработка политики безопасности
C. Проведение аудита процессов
D. Утверждение процедур контроля
3. Установите верную последовательность шагов защиты от утечки данных по техническим каналам:
A. Установка экранирующих устройств
B. Анализ технических каналов утечки
C. Тестирование защитных мер
D. Определение критических данных
4. Установите верную последовательность этапов настройки системы идентификации и аутентификации:
A. Выбор метода аутентификации
B. Определение пользователей системы
C. Настройка системы контроля доступа
D. Тестирование системы
5. Установите верную последовательность применения криптографических методов:
A. Шифрование данных при передаче
B. Генерация ключей шифрования
C. Выбор алгоритма шифрования
D. Тестирование безопасности

Вопросы на установление соответствия
1. Установите соответствие между этапами защиты от НСД и их характеристиками:
1. Анализ уязвимостей
2. Внедрение криптографии
3. Настройка аутентификации
4. Организационные меры
A. Разработка политики безопасности
B. Проверка подлинности пользователей
C. Выявление слабых мест системы
D. Защита данных при передаче
2. Установите соответствие между методами защиты от НСД и их описаниями:
1. Инженерно-технические меры
2. Организационные меры
3. Криптографические методы
4. Контроль доступа
A. Ограничение физического доступа
B. Шифрование данных
C. Обучение персонала
D. Настройка ролей пользователей
3. Установите соответствие между типами НСД и их характеристиками:
1. Физический доступ
2. Сетевой доступ
3. Программный доступ
4. Социальная инженерия
A. Взлом паролей через сеть
B. Обман пользователей
C. Проникновение в серверную
D. Использование вредоносного ПО
4. Установите соответствие между методами аутентификации и их описаниями:
1. Биометрическая

A. Использование смарт-карт
B. Сканирование отпечатков пальцев
C. Ввод секретного слова
D. Комбинация пароля и токена
5. Установите соответствие между криптографическими методами и их задачами:
1. Симметричное шифрование
2. Асимметричное шифрование
3. Хэширование
4. Цифровая подпись
A. Проверка целостности данных
B. Защита обмена ключами
C. Быстрое шифрование данных
D. Подтверждение авторства

Индикатор достижения компетенции Уметь
1. Выберите правильный ответ и обоснуйте свой выбор. Какой этап является первым при защите от НСД?
A. Внедрение криптографии
B. Определение объектов защиты
C. Настройка аутентификации
D. Тестирование системы
2. Выберите правильный ответ и обоснуйте свой выбор. Какой метод защиты предотвращает утечку по техническим каналам?
A. Обучение персонала
B. Установка экранирующих устройств
C. Парольная аутентификация
D. Анализ логов
3. Выберите правильный ответ и обоснуйте свой выбор. Что является основной целью криптографических методов?
A. Ускорение передачи данных
B. Обеспечение конфиденциальности
C. Управление доступом
D. Обучение пользователей
4. Выберите правильный ответ и обоснуйте свой выбор. Какая угроза НСД связана с обманом пользователей?
A. Физический доступ
B. Сетевой взлом
C. Социальная инженерия
D. Программный доступ
5. Выберите правильный ответ и обоснуйте свой выбор. Какой метод аутентификации использует смарт-карты?
A. Биометрический
B. Парольный
C. Токенный
D. Многофакторный
6. Выберите правильный ответ и обоснуйте свой выбор. Что относится к организационным мерам защиты?
A. Установка брандмауэра
B. Обучение персонала
C. Шифрование данных
D. Сканирование уязвимостей
7. Выберите правильный ответ и обоснуйте свой выбор. Какое свойство информации защищает шифрование?
A. Доступность
B. Целостность
C. Конфиденциальность
D. Аутентичность
8. Выберите правильный ответ и обоснуйте свой выбор. Кто отвечает за разработку политики защиты от НСД?
A. Системные администраторы
B. Руководство организации
C. Поставщики оборудования
D. Внешние консультанты
9. Выберите правильный ответ и обоснуйте свой выбор. Какой шаг является первым при настройке аутентификации?
A. Тестирование системы
B. Определение пользователей
C. Настройка ролей
D. Выбор метода
10. Выберите правильный ответ и обоснуйте свой выбор. Какой криптографический метод подтверждает авторство?
A. Симметричное шифрование
B. Хэширование
C. Асимметричное шифрование
D. Цифровая подпись

Индикатор достижения компетенции Владеть
1. Прочитайте текст и дайте развернутый ответ: Компания разрабатывает систему для хранения персональных данных клиентов. Необходимо защитить данные от НСД. Как внедрить меры защиты на этапе проектирования?

3. Прочитайте текст и дайте развернутый ответ: Компания обрабатывает конфиденциальные данные, требующие защиты от НСД. Как классифицировать данные и выбрать методы защиты?
4. Прочитайте текст и дайте развернутый ответ: Организация использует различные системы для передачи данных. Как оценить риски НСД и внедрить защитные меры?
5. Прочитайте текст и дайте развернутый ответ: Государственное учреждение хранит данные граждан. Какие организационные меры защиты от НСД следует внедрить?
6. Прочитайте текст и дайте развернутый ответ: Компания хочет защитить данные от утечек. Какие государственные органы могут помочь в разработке мер защиты?
7. Прочитайте текст и дайте развернутый ответ: Администратор заметил попытку НСД через сеть. Как провести анализ и устранить угрозу?
8. Прочитайте текст и дайте развернутый ответ: Компания получила угрозу утечки данных. Как оценить угрозу и подготовиться к последствиям?
9. Прочитайте текст и дайте развернутый ответ: Компания запускает платформу для онлайн-платежей. Какие меры защиты от НСД внедрить?
10. Прочитайте текст и дайте развернутый ответ: Сотрудник сообщил о компрометации пароля. Как расследовать и предотвратить повторение?

ОПК-14
Индикатор достижения компетенции Знать:
Вопросы на установление последовательности
1. Установите верную последовательность этапов разработки политики безопасности:
A. Реализация мер защиты
B. Анализ потребностей системы
C. Утверждение политики
D. Определение целей безопасности
2. Установите верную последовательность шагов настройки дискреционного доступа:
A. Назначение прав доступа
B. Определение субъектов
C. Настройка объектов защиты
D. Тестирование доступа
3. Установите верную последовательность этапов реализации мандатного доступа:
A. Определение уровней доступа
B. Назначение меток безопасности
C. Настройка контроля доступа
D. Анализ требований
4. Установите верную последовательность действий при создании парольной системы:
A. Настройка политики паролей
B. Определение пользователей
C. Тестирование системы
D. Выбор методов аутентификации
5. Установите верную последовательность этапов ролевой модели безопасности:
A. Назначение ролей пользователям
B. Определение ролей
C. Настройка прав ролей
D. Анализ задач системы
Вопросы на установление соответствия
1. Установите соответствие между этапами политики безопасности и их характеристиками:
1. Анализ потребностей
2. Определение целей
3. Реализация мер
4. Мониторинг политики
A. Постоянная проверка соблюдения
B. Внедрение технологий защиты
C. Выявление объектов защиты
D. Установление приоритетов
2. Установите соответствие между моделями доступа и их описаниями:
1. Дискреционный доступ
2. Мандатный доступ
3. Ролевой доступ
4. Тематический доступ
A. Управление по уровням секретности
B. Доступ по задачам пользователей
C. Доступ по ролям
D. Доступ по усмотрению владельца
3. Установите соответствие между аксиомами политики безопасности и их описаниями:
1. Аксиома целостности
2. Аксиома конфиденциальности
3. Аксиома доступности
4. Аксиома идентификации

2. Двухфакторная
3. Биометрическая
4. Многофакторная
A. Использование отпечатков пальцев
B. Пароль и токен
C. Только пароль
D. Комбинация трех методов
5. Установите соответствие между моделями безопасности и их задачами:
1. Субъектно-объектная
2. Ролевая
3. Теоретико-информационная
4. Мандатная
A. Управление по уровням доступа
B. Анализ потоков информации
C. Определение отношений доступа
D. Управление по ролям
Индикатор достижения компетенции Уметь
1. Выберите правильный ответ и обоснуйте свой выбор. Какой этап является первым при разработке политики безопасности?
A. Реализация мер защиты
B. Определение целей безопасности
C. Утверждение политики
D. Мониторинг соблюдения
2. Выберите правильный ответ и обоснуйте свой выбор. Какая модель доступа позволяет владельцу управлять правами?
A. Мандатная
B. Дискреционная
C. Ролевая
D. Тематическая
3. Выберите правильный ответ и обоснуйте свой выбор. Что является основной целью парольных систем?
A. Шифрование данных
B. Проверка подлинности
C. Управление ролями
D. Мониторинг угроз
4. Выберите правильный ответ и обоснуйте свой выбор. Какая аксиома политики безопасности защищает от изменения данных?
A. Конфиденциальность
B. Целостность
C. Доступность
D. Идентификация
5. Выберите правильный ответ и обоснуйте свой выбор. Какой метод используется в ролевой модели?
A. Назначение уровней секретности
B. Управление по ролям
C. Шифрование данных
D. Анализ потоков
6. Выберите правильный ответ и обоснуйте свой выбор. Что относится к мандатному доступу?
A. Управление по усмотрению владельца
B. Назначение ролей
C. Уровни секретности
D. Тематическое разделение
7. Выберите правильный ответ и обоснуйте свой выбор. Какое свойство обеспечивает непрерывность сервисов?
A. Конфиденциальность
B. Целостность
C. Доступность
D. Идентификация
8. Выберите правильный ответ и обоснуйте свой выбор. Кто отвечает за реализацию политики безопасности?
A. Пользователи системы
B. Руководство организации
C. Поставщики ПО
D. Внешние аудиторы
9. Выберите правильный ответ и обоснуйте свой выбор. Какой шаг является первым при настройке парольной системы?
A. Тестирование системы
B. Определение пользователей
C. Настройка политики паролей
D. Выбор методов аутентификации
10. Выберите правильный ответ и обоснуйте свой выбор. Какая модель анализирует потоки информации?
A. Ролевая
B. Мандатная
C. Теоретико-информационная
D. Дискреционная
Индикатор достижения компетенции Владеть

2. Прочитайте текст и дайте развернутый ответ: Организация обнаружила несанкционированный доступ. Как внедрить дискреционный доступ?
3. Прочитайте текст и дайте развернутый ответ: Компания хочет управлять доступом по ролям. Как внедрить ролевую модель?
4. Прочитайте текст и дайте развернутый ответ: Организация обрабатывает секретные данные. Как внедрить мандатный доступ?
5. Прочитайте текст и дайте развернутый ответ: Учреждение хранит данные граждан. Какие меры парольной защиты внедрить?
6. Прочитайте текст и дайте развернутый ответ: Компания хочет защитить данные. Какие органы могут помочь с политикой безопасности?
7. Прочитайте текст и дайте развернутый ответ: Администратор заметил нарушение доступа. Как расследовать и устранить проблему?
8. Прочитайте текст и дайте развернутый ответ: Компания получила угрозу нарушения политики безопасности. Как оценить угрозу?
9. Прочитайте текст и дайте развернутый ответ: Компания запускает CRM-систему. Как внедрить политику безопасности?
10. Прочитайте текст и дайте развернутый ответ: Сотрудник сообщил о слабом пароле. Как улучшить парольную систему?

ТЕСТОВЫЕ ЗАДАНИЯ К ЗАЧЕТУ

ОПК-4
1. Что такое шкала ценности информации? a) Оценка важности информации для организации b) Классификация угроз информационной безопасности c) Перечень мер защиты информации d) Список информационных ресурсов
2. Какой орган отвечает за контрразведывательную деятельность в области обеспечения информационной безопасности? a) ФСБ России b) ФСТЭК России c) Минцифры России d) Роскомнадзор
3. Что такое концепция комплексного обеспечения информационной безопасности? a) Применение только технических мер защиты информации b) Применение организационных и правовых мер защиты информации c) Применение организационных, правовых и технических мер защиты информации d) Применение только правовых мер защиты информации
4. Какой нормативный акт регулирует деятельность в области информационной безопасности РФ? a) Доктрина информационной безопасности РФ b) Федеральный закон "О безопасности" c) Федеральный закон "Об информации, информационных технологиях и о защите информации" d) Указ Президента РФ "О стратегии национальной безопасности РФ"
5. Что такое неформальная модель нарушителя? a) Описание типичных мотивов, целей и методов нарушителя информационной безопасности b) Классификация уязвимостей информационной системы c) Перечень угроз информационной безопасности d) Методика оценки рисков
6. Как обычно классифицируются угрозы информационной безопасности? a) По источнику, типу и степени риска b) По степени сложности реализации c) По используемым технологиям d) По целям реализации угрозы
7. Что является основной целью проведения анализа уязвимостей? a) Выявление слабых мест в системе защиты информации b) Разработка новых методов защиты информации c) Классификация угроз информационной безопасности d) Оценка эффективности существующих мер защиты
8. Какой из перечисленных вариантов наиболее точно описывает цель неформальной модели нарушителя? a) Классификация уязвимостей системы b) Описание типичной модели поведения злоумышленника c) Разработка новых методов защиты информации d) Оценка эффективности существующих мер защиты
9. Какой из перечисленных методов наиболее эффективен для защиты от угрозы кражи данных? a) Использование брандмауэров b) Шифрование данных c) Регулярное резервное копирование d) Установка антивирусного ПО
10. Что из перечисленного не относится к методам реализации угроз информационной безопасности? a) Эксплуатация уязвимостей b) Социальная инженерия c) Физическое проникновение d) Применение средств криптографической защиты
11. Что из перечисленного не относится к методам защиты от несанкционированного доступа? a) Идентификация и аутентификация пользователей b) Разграничение доступа c) Аудит действий пользователей d) Обновление антивирусных баз
12. Какой из перечисленных вариантов наиболее точно описывает цель анализа уязвимостей? a) Классификация угроз информационной безопасности b) Разработка новых методов защиты информации c) Выявление слабых мест в системе защиты информации d) Оценка эффективности существующих мер защиты
13. Какая из перечисленных угроз относится к нарушению доступности информационных ресурсов? a) Фишинговая атака b) Атака "человек посередине" c) Отказ в обслуживании (DoS-атака) d) Вирус-вымогатель
14. Что из перечисленного не входит в задачи анализа рисков информационной безопасности? a) Идентификация активов b) Оценка уязвимостей c) Определение вероятности реализации угроз d) Разработка политики информационной безопасности
15. Какой из перечисленных факторов наиболее важен при оценке угрозы нарушения конфиденциальности информации? a) Объем информационных ресурсов b) Сложность реализации угрозы c) Ценность конфиденциальной информации d) Наличие инсайдерской угрозы

ОПК-14
1. Что не относится к формам представления информации? а) Текстовая б) Числовая в) Графическая г) Открытая
2. Какой орган не занимается обеспечением информационной безопасности в России? а) ФСБ б) ФСТЭК в)

ОПК-14
1. Что такое мандатная политика доступа? а) Политика доступа, основанная на ролях и уровнях секретности б) Политика доступа, управляемая собственником объекта в) Политика, при которой пользователь может сам настраивать права доступа г) Политика, основанная на разрешениях для каждого действия
2. Что такое теоретико-информационная модель безопасности? а) Модель, основанная на информационной энтропии б) Модель, использующая математическую теорию информации в) Модель, описывающая угрозы информационной безопасности г) Модель, основанная на ролевой парадигме доступа
3. В чем заключается ролевая модель безопасности? а) Разграничение доступа на основе присвоенных ролей б) Использование паролей для аутентификации в) Применение цифровых сертификатов г) Шифрование данных при передаче
4. Что не относится к видам информационных войн? а) Информационно-техническая б) Информационно-психологическая в) Кибервойна г) Экономическая война
5. Что такое информационно-техническая война? а) Ведение боевых действий с использованием информационных технологий б) Применение технических средств для нарушения работы систем противника в) Информационное противоборство в киберпространстве г) Психологическое воздействие на население
6. На каком уровне осуществляется семантическая защита информации? а) Физический уровень б) Уровень представления данных в) Уровень содержания информации г) Уровень приложений
7. Что является основной задачей парольных систем разграничения доступа? а) Защита конфиденциальности

6.5. Примерная тематика курсовых работ (проектов)

Учебным планом не предусмотрено

6.6. Методические указания для обучающихся по освоению дисциплины (модуля)

Методические рекомендации по подготовке к лекционным занятиям

Просмотрите конспект сразу после занятий. Пометьте материал конспекта лекций, который вызывает затруднения для понимания. Попытайтесь найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь на текущей консультации или на ближайшей лекции за помощью к преподавателю. Каждую неделю рекомендуется отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам.
Работа с рекомендованной литературой:
При работе с основной и дополнительной литературой целесообразно придерживаться такой последовательности. Сначала прочитать весь заданный текст в быстром темпе. Цель такого чтения заключается в том, чтобы создать общее представление об изучаемом материале, понять общий смысл прочитанного. Затем прочитать вторично, более медленно, чтобы в ходе чтения понять и запомнить смысл каждой фразы, каждого положения и вопроса в целом. Чтение приносит пользу и становится продуктивным, когда сопровождается записями. Это может быть составление плана прочитанного текста, тезисы или выписки, конспектирование и др. Выбор вида записи зависит от характера изучаемого материала и целей работы с ним. Если содержание материала несложное, легко усваиваемое, можно ограничиться составлением плана. Если материал содержит новую и трудно усваиваемую информацию, целесообразно его законспектировать. План – это схема прочитанного материала, перечень вопросов, отражающих структуру и последовательность материала. Конспект – это систематизированное, логичное изложение материала источника. Различаются четыре типа конспектов: - план-конспект – это развернутый детализированный план, в котором по наиболее сложным вопросам даются подробные пояснения, - текстуальный конспект – это воспроизведение наиболее важных положений и фактов источника, - свободный конспект – это четко и кратко изложенные основные положения в результате глубокого изучения материала, могут присутствовать выписки, цитаты, тезисы; часть материала может быть представлена планом, - тематический конспект – составляется на основе изучения ряда источников и дает ответ по изучаемому вопросу. В процессе изучения материала источника и составления конспекта нужно обязательно применять различные выделения, подзаголовки, создавая блочную структуру конспекта. Это делает конспект легко воспринимаемым и удобным для работы.

Методические рекомендации по подготовке к практическим занятиям

Практические занятия представляют особую форму сочетания теории и практики. Их назначение – углубление проработки теоретического материала предмета путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к практическим занятиям включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение практического занятия предполагает, например:
- индивидуальные выступления студентов с сообщениями по какому-либо вопросу изучаемой темы;
- фронтальное обсуждение рассматриваемой проблемы, обобщения и выводы;
- решение задач и упражнений по образцу;
- решение вариантных задач и упражнений;
- решение ситуационных производственных (профессиональных) задач;
- проектирование и моделирование разных видов и компонентов профессиональной деятельности;
- выполнение контрольных работ;
- работу с тестами.
При подготовке к практическим занятиям студентам рекомендуется: внимательно ознакомиться с тематикой практического занятия; прочесть конспект лекции по теме, изучить рекомендованную литературу; составить краткий план ответа на каждый вопрос практического занятия; проверить свои знания, отвечая на вопросы для самопроверки; если встретятся незнакомые термины, обязательно обратиться к словарю и зафиксировать их в тетради. Все письменные задания выполнять в рабочей тетради. Практические занятия развивают у студентов навыки самостоятельной работы по решению конкретных

задач.

Методические рекомендации по подготовке к лабораторным работам

Лабораторные работы представляют одну из форм освоения теоретического материала с одновременным формированием практических навыков в изучаемой дисциплине (модуле). Их назначение – углубление проработки теоретического материала, формирование практических навыков путем регулярной и планомерной самостоятельной работы студентов на протяжении всего курса. Процесс подготовки к лабораторным работам включает изучение нормативных документов, обязательной и дополнительной литературы по рассматриваемому вопросу. Непосредственное проведение лабораторной работы предполагает:
- изучение теоретического материала по теме лабораторной работы (по вопросам изучаемой темы);
- выполнение необходимых расчетов и экспериментов;
- оформление отчета с заполнением необходимых таблиц, построением графиков, подготовкой выводов по проделанным экспериментам и теоретическим расчетам;
- по каждой лабораторной работе проводится контроль: проверяется содержание отчета, проверяется усвоение теоретического материала.
Контроль усвоения теоретического материала является индивидуальным.

Методические указания по выполнению отчёта к лабораторным работам

Основным требованием по выполнению лабораторных и практических работ является полное исчерпывающее описание всей проделанной работы, позволяющее судить о полученных результатах, степени выполнения и профессиональной подготовки студентов.
Методические указания обеспечивают комплексный подход в учебной работе студентов, единство и преемственность требований к оформлению результатов работы на разных этапах обучения. С единых позиций приведены основные требования к структуре, оформлению и содержанию отчета по лабораторным и практическим работам.
Структура отчёта:
- цель работы;
- краткие теоретические сведения;
- ход выполнения работы;
- выводы.
Дополнительные элементы:
- приложения;
- библиографический список.
Требования к содержанию отчёта:
1. Титульный лист
В верхнем поле листа указывают полное наименование учебного заведения.
В среднем поле указывается вид работы, в данном случае лабораторная или практическая работа с указанием курса, по которому она выполнена, и ниже ее название. Название работы приводится без слова "тема" и в кавычки не заключается.
Далее ближе к правому краю титульного листа указывают фамилию, инициалы и группу учащегося, выполнившего работу, а также фамилию, инициалы преподавателя, принявшего работу.
В нижнем поле листа указывается место выполнения работы и год ее написания (без слова год).
2. Цель работы должна отражать тему работы, а также конкретные задачи, поставленные студенту на период выполнения работы. По объему цель работы в зависимости от сложности и многозадачности работы составляет от нескольких строк до 0,5 страницы.
3. Краткие теоретические сведения. В этом разделе излагается краткое теоретическое описание изучаемой в работе темы. Материал раздела не должен копировать содержание методического пособия или учебника по данной теме, а ограничивается изложением основных понятий, требующихся для дальнейшей обработки полученных результатов. Объем литературного обзора не должен превышать 1/3 части всего отчета.
4. Ход выполнения работы. В данном разделе подробно излагается методика выполнения работы, процесс получения данных и способ их обработки. Если используются стандартные пакеты компьютерных программ для обработки экспериментальных результатов, то необходимо обосновать возможность и целесообразность их применения, а также подробности обработки данных с их помощью.
5. Выводы по работе - кратко излагаются результаты работы, полученные в результате выполнения работы, а также краткий анализ полученных результатов.
Отчет по лабораторной работе оформляется на листе формата А4. Допускается оформление отчета по лабораторной работе в электронном виде средствами Microsoft Office. Текст работы должен быть напечатан через полтора интервала шрифтом Times New Roman, кегль – 12. Поля должны оставаться по всем четырем сторонам печатного листа: левое – не менее 30 мм, правое – не менее 10, нижнее – не менее 20 и верхнее – не 15 мм.
Для защиты лабораторной работы студент должен подготовить отчет, провести самостоятельную работу, иметь отметку о проверенном отчете.
Результаты определяются по пятибалльной системе оценок.

Методические рекомендации по выполнению реферата

Реферат – письменная работа объемом 8–10 страниц. Это краткое и точное изложение сущности какого-либо вопроса, темы. Тему реферата студент выбирает из предложенных преподавателем или может предложить свой вариант. В реферате нужны развернутые аргументы, рассуждения, сравнения. Содержание темы излагается объективно от имени автора. Функции реферата: информативная, поисковая, справочная, сигнальная, коммуникативная. Степень выполнения этих

функций зависит от содержательных и формальных качеств реферата и для каких целей их использует. Требования к языку реферата: должен отличаться точностью, краткостью, ясностью и простотой.
Структура реферата:
1. Титульный лист
2. Оглавление (на отдельной странице). Указываются названия всех разделов (пунктов плана) реферата и номера страниц, указывающие начало этих разделов в тексте реферата.
3. Введение. Аргументируется актуальность исследования, т.е. выявляется практическое и теоретическое значение данного исследования. Далее констатируется, что сделано в данной области предшественниками, перечисляются положения, которые должны быть обоснованы. Обязательно формулируются цель и задачи реферата.
4. Основная часть. Подчиняется собственному плану, что отражается в разделении текста на главы, параграфы, пункты. План основной части может быть составлен с использованием различных методов группировки материала. В случае если используется чья-либо неординарная мысль, идея, то обязательно нужно сделать ссылку на того автора, у кого взят данный материал.
5. Заключение. Последняя часть научного текста. В краткой и сжатой форме излагаются полученные результаты, представляющие собой ответ на главный вопрос исследования.
6. Приложение. Может включать графики, таблицы, расчеты.
7. Библиография (список литературы). Указывается реально использованная для написания реферата литература. Названия книг располагаются по алфавиту с указанием их выходных данных. Общие требования к построению, содержанию и оформлению».
При проверке реферата оцениваются:
- знание фактического материала, усвоение общих представлений, понятий, идей;
- характеристика реализации цели и задач исследования;
- степень обоснованности аргументов и обобщений;
- качество и ценность полученных результатов;
- использование литературных источников;
- культура письменного изложения материала;
- культура оформления материалов работы.
Правила написания научных текстов (реферат):
Здесь приводятся рекомендации по консультированию студентов относительно данного вида самостоятельной работы. Во время консультаций руководителю следует предложить к обсуждению следующие вопросы.
• Какова истинная цель Вашего научного текста – это поможет Вам разумно распределить свои силы и время.
• Важно разобраться, кто будет «читателем» Вашей работы.
• Начинать писать серьезную работу следует не раньше, чем возникнет ощущение, что по работе с источниками появились идеи, которыми можно поделиться.
• Должна быть идея, а для этого нужно научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного).
• Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно, а также стремясь структурировать свой текст.
• Объем текста и различные оформительские требования во многом зависят от принятых в конкретном учебном заведении порядков.

Методические рекомендации по выполнению контрольных работ

Контрольная работа выполняется по вариантам. На бланке указывается факультет, курс, группа, ФИО студента. Вопросы строятся на основе тестовых и ситуативных заданий. В тестовых заданиях, выбирается правильный(ые) ответ(ы). При решении ситуативных заданий выбирается правильная последовательность действий в рассматриваемой ситуации. Проверка контрольной работы позволяет выявить и исправить допущенные студентами ошибки, указать, какие вопросы дисциплины (модуля) ими недостаточно усвоены и требуют доработки. Студент должен внимательно ознакомиться с письменными замечаниями преподавателя и приступить к их исправлению, для чего еще раз повторить соответствующий материал.

Методические рекомендации по подготовке к коллоквиуму

Коллоквиумом называется собеседование преподавателя и студента по заранее определенным контрольным вопросам. Целью коллоквиума является формирование у студента навыков анализа теоретических проблем на основе самостоятельного изучения учебной и научной литературы. На коллоквиум выносятся крупные, проблемные, нередко спорные теоретические вопросы. Упор делается на монографические работы профессора-автора данного спецкурса. От студента требуется:
- владение изученным в ходе учебного процесса материалом, относящимся к рассматриваемой проблеме;
- знание разных точек зрения, высказанных в научной литературе по соответствующей проблеме, умение сопоставлять их между собой;
- наличие собственного мнения по обсуждаемым вопросам и умение его аргументировать.
Коллоквиум - это не только форма контроля, но и метод углубления, закрепления знаний студентов, так как в ходе собеседования преподаватель разъясняет сложные вопросы, возникающие у студента в процессе изучения данного источника. Однако коллоквиум не консультация и не экзамен. Его задача добиться глубокого изучения отобранного материала, пробудить у студента стремление к чтению дополнительной социологической литературы. Подготовка к коллоквиуму начинается с установочной консультации преподавателя, на которой он разъясняет развернутую тематику проблемы, рекомендует литературу для изучения и объясняет процедуру проведения коллоквиума. Как правило, на

самостоятельную подготовку к коллоквиуму студенту отводится 3-4 недели. Методические указания состоят из рекомендаций по изучению источников и литературы, вопросов для самопроверки и кратких конспектов ответа с перечислением основных фактов и событий, относящихся к пунктам плана каждой темы. Это должно помочь студентам целенаправленно организовать работу по овладению материалом и его запоминанию. При подготовке к коллоквиуму следует, прежде всего, просмотреть конспекты лекций и практических занятий и отметить в них имеющиеся вопросы коллоквиума. Если какие-то вопросы вынесены преподавателем на самостоятельное изучение, следует обратиться к учебной литературе, рекомендованной преподавателем в качестве источника сведений.
Коллоквиум проводится в форме индивидуальной беседы преподавателя с каждым студентом или беседы в небольших группах (2-3 человека). Обычно преподаватель задает несколько кратких конкретных вопросов, позволяющих выяснить степень добросовестности работы с литературой, проверяет конспект. Далее более подробно обсуждается какая-либо сторона проблемы, что позволяет оценить уровень понимания. По итогам коллоквиума выставляется дифференцированная оценка по пятибалльной системе.

Методические рекомендации по устному опросу/самоподготовке

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется, используя лист опорных сигналов,
воспроизвести по памяти определения, выводы формул, формулировки основных положений и доказательств. В случае необходимости следует рекомендовать еще раз внимательно разобраться в материале. Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение решать задачи или пройти тестирование по пройденному материалу. Однако преподавателю следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

Методические рекомендации по подготовке к семинарским занятиям

Одним из видов внеаудиторной самостоятельной работы является подготовка к семинарским занятиям. Семинар – форма учебно-практических занятий, при которой студенты обсуждают сообщения, доклады и рефераты, выполненные ими по результатам учебных или научных исследований под руководством преподавателя. Преподаватель в этом случае является координатором обсуждений темы семинара, подготовка к которому является обязательной. Поэтому тема семинара и основные источники обсуждения предъявляются до обсуждения для детального ознакомления, изучения. Цели обсуждений направлены на формирование навыков профессиональной полемики и закрепление обсуждаемого материала. Семинар – это такая форма организации обучения, при которой на этапе подготовки доминирует самостоятельная работа учащихся с учебной литературой и другими дидактическими средствами над серией вопросов, проблем и задач, а в процессе семинара идут активное обсуждение, дискуссии и выступления учащихся, где они под руководством преподавателя делают обобщающие выводы и заключения. Семинар предназначен для углубленного изучения дисциплины, овладения методологией научного познания, то главная цель семинарских занятий – обеспечить студентам возможность овладеть навыками и умениями использования теоретического знания применительно к особенностям изучаемой отрасли.

Методические рекомендации по подготовке к эссе

Одним из видов самостоятельной работы студентов является написание творческой работы по заданной либо согласованной с преподавателем теме. Творческая работа (эссе) представляет собой оригинальное произведение объемом 500-700 слов, посвященное какой-либо значимой классической либо современной проблеме в определенной теоретической и практической области. Творческая работа не является рефератом и не должна носить описательный характер, большое место в ней должно быть уделено аргументированному представлению своей точки зрения студентами, критической оценке рассматриваемого материала и проблематики, что должно способствовать раскрытию творческих и аналитических способностей. Цели написания эссе – научиться логически верно и аргументировано строить устную и письменную речь; работать над углублением и систематизацией своих философских знаний; овладеть способностью использовать основы знаний для формирования мировоззренческой позиции. Приступая к написанию эссе, изложите в одном предложении, что именно вы будете утверждать и доказывать (свой тезис).

Методические рекомендации по подготовке к докладу

Для подготовки доклада необходимо выбрать актуальную тему. Желательно, чтобы тема была интересна докладчику и вызывала желание качественно подготовить материалы. Подготовка доклада предполагает: определение цели доклада; подбор необходимого материала, определяющего содержание доклада; составление плана доклада, распределение собранного материала в необходимой логической последовательности.
Композиция доклада имеет вступление, основную часть и заключение.
Вступление должно содержать: название доклада; сообщение основной идеи; современную оценку предмета изложения; краткое перечисление рассматриваемых вопросов; интересную для слушателей форму изложения. Основная часть, в которой необходимо раскрыть суть темы, обычно строится по принципу отчёта. Задача основной части: представить достаточно данных для того, чтобы слушатели заинтересовались темой.
Заключение – чёткое обобщение и краткие выводы по излагаемой теме.

Методические рекомендации по подготовке к собеседованию

Собеседование – средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.
Цель собеседования: проверка усвоения знаний; умений применять знания; сформированности профессионально значимых личностных качеств.
Подготовка к собеседованию предполагает повторение пройденного материала и приобретение навыка свободного владения терминологией и фактическими данными по определенному разделу дисциплины (модуля).

Методические рекомендации по подготовке к тестированию/ итоговому тестированию

Тестирование/итоговое тестирование – это система стандартизированных заданий, определенного содержания и упорядоченных в рамках определенной стратегии предъявления, позволяющая качественно оценить структуру и эффективно измерить уровень знаний, умений и навыков по дисциплине (модулю). Тестирование позволяет оценить у студентов уровень знаний фактического материала, умения логически мыслить, способности к рефлексии и творческому подходу к решению поставленной задачи на каждом этапе их обучения.
При самостоятельной подготовке к тестированию студенту необходимо:
- четко выяснить все условия тестирования заранее (сколько тестов будет предложено, сколько времени отводится на тестирование, какова система оценки результатов);
- проконсультироваться с преподавателем по вопросу выбора учебной литературы;
- проработать информационный материал по разделу дисциплине;
- конспективно выписать из соответствующих разделов учебной дисциплины основные понятия, ключевые идеи, теоретические концепции и подходы;
- повторить теоретический материал лекций, самостоятельно изученной учебной и научной литературы, семинарских занятий.
При выполнении тестовых заданий рекомендуется:
- внимательно полностью прочитать вопрос и предлагаемые варианты ответов, выбрать правильные из них (их может быть несколько);
- при затруднении при ответе на сложный для студента вопрос целесообразно переходить к другим вопросам теста. По завершению ответов на все последующие вопросы теста необходимо вернуться к трудному вопросу и дать на него продуманный ответ;
- по окончании тестирования следует проверить правильность данных ответов на вопросы теста, чтобы избежать механических ошибок.

Методические рекомендации по подготовке к экзамену

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению практических задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной дисциплине (модулю). Экзаменационная сессия – это серия экзаменов, установленных учебным планом. Между экзаменами интервал 2-4 дня, в течение студент систематизирует уже имеющиеся знания. На консультации перед экзаменом студенты должны быть ознакомлены с основными требованиями и получить ответы на возникающие в процессе подготовки
вопросы. Необходимо ориентировать студентов на систематическую подготовку к занятиям в течение семестра, что позволит использовать время экзаменационной сессии для
систематизации знаний.

Методические рекомендации по подготовке к зачету/зачету с оценкой

В ходе подготовки к зачету/зачету с оценкой студент, в первую очередь, должен систематизировать знания, полученные в ходе изучения дисциплины. К зачету/зачету с оценкой необходимо готовиться целенаправленно, регулярно, систематически и с первых дней обучения по данной дисциплине (модулю). В самом начале учебного курса познакомьтесь со следующей учебно-методической документацией:
- программой дисциплины (модуля);
- перечнем знаний, умений и навыков, которыми студент должен владеть;
- тематическими планами лекций, семинарских занятий;
- учебниками, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к зачету/зачету с оценкой.
После этого у обучающихся должно сформироваться четкое представление об объеме и характере знаний и умений, которыми надо будет овладеть по дисциплине (модулю). Систематическое выполнение учебной работы на лекциях и лабораторных занятиях позволит успешно освоить дисциплину (модуль) и создать хорошую базу для сдачи зачета/зачета с оценкой.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература	
7.1.1. Основная литература	
Л.1.1	Медведев В.А. Информационная безопасность. Введение в специальность + еПриложение:Тесты [Электронный ресурс]:Учебник. - Москва: КноРус, 2024. - 143 с. – Режим доступа: https://book.ru/book/951878

Л.1.2	Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]:учебник для вузов. - Санкт-Петербург: Лань, 2023. - 124 с. – Режим доступа: https://e.lanbook.com/book/293009
Л.1.3	Мельников В.П., Куприянов А.И., Васильева Т.Ю., Мельников В.П. Информационная безопасность [Электронный ресурс]:Учебник. - Москва: КноРус, 2023. - 371 с. – Режим доступа: https://book.ru/book/950148
Л.1.4	Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность. Лабораторный практикум + еПриложение [Электронный ресурс]:Учебное пособие. - Москва: КноРус, 2023. - 131 с. – Режим доступа: https://book.ru/book/949452
Л.1.5	О.В. Прохорова Информационная безопасность и защита информации:учебник. - СПб.: Лань, 2023. - 124 с.: ил.
7.2. Лицензионное и свободно распространяемое программное обеспечение в том числе отечественного производства	
7.2.1	Microsoft Windows 10
7.2.2	Kaspersky Endpoint Security
7.2.3	Microsoft Office 2013 Standard
7.2.4	Microsoft Visual Studio Professional 2017
7.2.5	Virtualbox
7.2.6	Веб-сервер OpenServer
7.2.7	Microsoft Visual Code
7.2.8	Qt Creator
7.2.9	Notepad ++
7.2.10	Microsoft®WINHOME 10 Russian Academic OLP lLicense NoLevel Legalization GetGenuine
7.3. Перечень профессиональных баз данных, информационных справочных систем и ресурсов сети Интернет	
7.3.1	Электронно-библиотечная система "Лань". Режим доступа: https://e.lanbook.com/
7.3.2	Электронно-библиотечная система "Университетская библиотека онлайн". Режим доступа: https://biblioclub.ru/
7.3.3	Электронно-библиотечная система "BOOK.ru". Режим доступа: https://book.ru/
7.3.4	Сайт национального открытого университета "ИНТУИТ". Режим доступа: https://intuit.ru/
7.3.5	ПЛАТФОРМА ОНЛАЙН-ОБРАЗОВАНИЯ «РАЗУМ». Режим доступа: https://razoom.mgutm.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1	Адрес: 344002, Ростовская область, г. Ростов-на-Дону, пер. Семашко, д. 55: аудитория 20-28 - Компьютерный класс : 15 персональных компьютеров, объединённых в локальную вычислительную сеть на базе выделенного сервера приложений и web-сервера, наглядными пособиями, Мультимедийная установка «Toshiba» с экраном 3,5 м. Лицензионные программы:. ПО ОС Windows XP professional, MS Office 2003. Microsoft Visual Studio 2010-2013. Opera, Mozilla Firefox, Adobe Acrobat Reader 3.01,. WinDjView, КОМПАС-3D LT, 1С Предприятие 8.1, Система для моделирования бизнеса и оценки бизнес-проектов «Project Expert 7 ─ Эксперт Системс» (сетевая версия). CorelDRAW Graphics Suite X7. GRAPHISOFT ArchiCAD 15, Autodesk DWG Viewer, AVS DVD Player 2.4, CorelDraw Graphics Suite X4, Google SketchUp6.7, QuickTime, QBacic, Pascal, Delphi, Kaspersky Endpoint Security. IQlib. Все компьютеры подключены к сети Internet

9. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Организация образовательного процесса для лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Методическими рекомендациями по организации образовательного процесса для инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса» Министерства образования и науки РФ от 08.04.2014г. № АК-44/05вн. В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала. Подбор и разработка учебных материалов производится с учетом индивидуальных особенностей. Предусмотрена возможность обучения по индивидуальному графику, при составлении которого возможны различные варианты проведения занятий: в академической группе и индивидуально, на дому с использованием дистанционных образовательных технологий.

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Физика, математика и информационные технологии
Протокол от __ _____ 2027 г. № __
Зав. кафедрой Нечушкин Александр Юрьевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Пищевые технологии и оборудование
Протокол от __ _____ 2027 г. № __
Зав. кафедрой Павлова Ирина Васильевна _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Физика, математика и информационные технологии
Протокол от __ _____ 2028 г. № __
Зав. кафедрой Нечушкин Александр Юрьевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Пищевые технологии и оборудование
Протокол от __ _____ 2028 г. № __
Зав. кафедрой Павлова Ирина Васильевна _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Физика, математика и информационные технологии
Протокол от __ _____ 2029 г. № __
Зав. кафедрой Нечушкин Александр Юрьевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Пищевые технологии и оборудование
Протокол от __ _____ 2029 г. № __
Зав. кафедрой Павлова Ирина Васильевна _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
_____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Физика, математика и информационные технологии
Протокол от __ _____ 2030 г. № __
Зав. кафедрой Нечушкин Александр Юрьевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Пищевые технологии и оборудование
Протокол от __ _____ 2030 г. № __
Зав. кафедрой Павлова Ирина Васильевна _____