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)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

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

УТВЕРЖДАЮ
И.о. директора ДКГИПТиБ (филиала)
Г.В. Павлятенко
«10» апреля 2026 г.

Рабочая программа дисциплины (модуля)

Б1.О.04.12 ОБЩЕПРОФЕССИОНАЛЬНЫЙ МОДУЛЬ Информационная безопасность

Кафедра:	Физика, математика и информационные технологии
Направление подготовки:	09.03.03 Прикладная информатика
Направленность (профиль):	Управление проектами в области информационных технологий
Квалификация выпускника:	Бакалавр
Форма обучения:	очно-заочная
Год набора:	2026
Общая трудоемкость:	216 часов/6 з.е.

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 09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922),

Руководитель ОПОП
канд.экон.наук,доцент Левчук В.В._____ ___

Рабочая программа обсуждена на заседании обеспечивающей кафедры
Физика, математика и информационные технологии
Протокол от 30 июня 2026 г. № 11
И.о.зав. кафедрой Левчук Валерия Владимировна_____

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 ОСНОВНОЙ ПРОФЕССИОНАЛЬНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ И ОБЪЕМ С РАСПРЕДЕЛЕНИЕМ ПО СЕМЕСТРАМ

Цикл (раздел) ОП: "Информационная безопасность"

Дисциплина относится к обязательной части ОПОП и обязательна для освоения.

Связь с предшествующими дисциплинами (модулями), практиками

№ п/п	Наименование	Семестр	Шифр компетенции
1	Информационно-коммуникационные технологии	5	ОПК-3.1, ОПК-3.2, ОПК-3.3

Распределение часов дисциплины

Семестр (<Курс>.<Семестр на курсе>)	6 (3.2)		7 (4.1)		Итого	
Недель	13 4/6		17 1/6			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	4	4	8	8	12	12
Лабораторные			8	8	8	8
Практические	4	4	8	8	12	12
В том числе электрон.	8	8	60	60	68	68
В том числе в форме практ.подготовки			2		2	
Итого ауд.	8	8	24	24	32	32
Контактная работа	8	8	24	24	32	32
Сам. работа	64	64	84	84	148	148
Часы на контроль			36	36	36	36
Итого	72	72	144	144	216	216

Вид промежуточной аттестации:

Зачёт 6 семестр

Экзамен 7 семестр

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-3:Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ОПК-3.1: Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.2: Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.3: Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименования разделов, тем, их краткое содержание и результаты освоения /вид занятия/	Семестр	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/**	6	16	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы к самоподготовке
1.2	**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 Уметь: Анализировать и классифицировать информацию; Оценивать ценность информации; Разрабатывать стратегии защиты информации; Применять правовые нормы Владеть: Навыками оценки и классификации информации;**	6	16	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы к самоподготовке

	Техниками защиты информации; Инструментами анализа информационных ресурсов /Ср/						
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; Коммуникационными навыками /Ср/**	6	16	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы к самоподготовке
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**	6	16	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы к самоподготовке

	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/						
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; 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/**	7	21	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы к самоподготовке
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**	7	21	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы к самоподготовке

	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/						
1.7	**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 Уметь: Проектировать и реализовывать политику безопасности для различных типов информационных систем; Применять субъектно-объектные**	7	21	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы к самоподготовке

	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/						
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 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/**	7	21	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы к самоподготовке
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**	6	1	0	0	ОПК-3.1	устный опрос, тестирование

	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 /Лек/						
1.10	**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/**	6	1	0	0	ОПК-3.1	устный опрос, тестирование
1.11	**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 /Лек/**	6	1	0	0	ОПК-3.1	устный опрос, тестирование
1.12	**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**	6	1	0	0	ОПК-3.1	устный опрос, тестирование

	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/						
1.13	**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 /Лек/**	7	2	0	0	ОПК-3.1	устный опрос, тестирование
1.14	**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 /Лек/**	7	2	0	0	ОПК-3.1	устный опрос, тестирование
1.15	**Тема 7. Политика и модели безопасности Краткое содержание: Политика безопасности. Субъектно-объектные модели разграничения доступа. Аксиомы политики**	7	2	0	0	ОПК-3.1	устный опрос, тестирование

	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 /Лек/						
1.16	**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/**	7	2	0	0	ОПК-3.1	устный опрос, тестирование
1.17	**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. 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/**	6	2	0	0	ОПК-3.2,ОПК-3.3	отчет по практической работе
1.18	**Тема 4. Угрозы информационной безопасности Краткое содержание:**	6	2	0	0	ОПК-3.2,ОПК-3.3	отчет по практической работе

	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/						
1.19	**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 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**	7	8	0	0	ОПК-3.2,ОПК-3.3	отчет по практической работе

	правилам безопасного использования информационных ресурсов и соблюдения политики безопасности /Пр/						
1.20	**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/**	7	4	0	0	ОПК-3.2,ОПК-3.3	отчет по лабораторной работе
1.21	**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 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**	7	4	0	0	ОПК-3.2,ОПК-3.3	отчет по лабораторной работе

	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, 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;**	6	0	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы к зачету, тестирование

	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 Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности Владеть: навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности /Экзамен/**	7	36	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы к экзамену, тестирование

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-3:Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

Недостаточный уровень:

Знания принципов, методов и средств решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности не сформированы

Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности не сформировано

Владение навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности не сформировано

Пороговый уровень:

Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной

Умеет решать стандартные задачи профессиональной деятельности на основе информационной

Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

Продвинутый уровень:

Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры

Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры

Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций

Высокий уровень:

Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

6.2. Описание критериев оценивания успеваемости

НЕДОСТАТОЧНЫЙ УРОВЕНЬ Обучающийся демонстрирует:	ПОРОГОВЫЙ УРОВЕНЬ Обучающийся демонстрирует:	ПРОДВИНУТЫЙ УРОВЕНЬ Обучающийся демонстрирует:	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.	- 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.	- 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.	- 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 3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности

1. Что такое государственная политика информационной безопасности?
2. Каковы основные цели и задачи государственной политики информационной безопасности?
3. Какие существуют нормативные правовые акты в области информационной безопасности?
4. Что такое концепция комплексного обеспечения информационной безопасности?
5. Каковы основные направления обеспечения информационной безопасности?
6. Что такое система органов обеспечения информационной безопасности?
7. Какие существуют уровни обеспечения информационной безопасности?
8. Что такое межгосударственное сотрудничество в области информационной безопасности?

9. Что такое международные стандарты в области информационной безопасности?
10. Какие существуют основные проблемы в области обеспечения информационной безопасности?
Тема 4. Угрозы информационной безопасности
1. Что такое угроза информационной безопасности?
2. Какие существуют источники угроз информационной безопасности?
3. Что такое внутренние угрозы информационной безопасности?
4. Что такое внешние угрозы информационной безопасности?
5. Что такое техногенные угрозы информационной безопасности?
6. Что такое стихийные угрозы информационной безопасности?
7. Каковы основные виды компьютерных атак?
8. Что такое вредоносное программное обеспечение?
9. Что такое социальная инженерия в контексте информационной безопасности?
10. Какие существуют методы анализа и оценки угроз информационной безопасности?
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?
Тема 7. Политика и модели безопасности
1. Что такое политика безопасности?
2. Какие существуют виды политик безопасности?
3. Что такое модель безопасности?
4. Какие существуют основные модели безопасности?
5. Что такое мандатное управление доступом?
6. Что такое дискреционное управление доступом?
7. Что такое принцип минимальных привилегий?
8. Что такое принцип разделения обязанностей?
9. Какова роль политик и моделей безопасности в обеспечении информационной безопасности?
10. Какие существуют проблемы и ограничения в применении политик и моделей безопасности?
Тема 8. Информационные войны и информационное противоборство
1. Что такое информационная война?
2. Какие существуют формы и методы ведения информационной войны?
3. Что такое информационное оружие?
4. Что такое информационно-психологическое воздействие?
5. Что такое информационное противоборство?
6. Какова роль средств массовой информации в информационном противоборстве?
7. Что такое кибертерроризм?
8. Что такое хактивизм?
9. Какие существуют международные конвенции и соглашения в области информационной безопасности?
10. Какие существуют меры противодействия информационным войнам и информационному противоборству?

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 3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности
1. Какой орган является координатором деятельности по обеспечению информационной безопасности в РФ? а) ФСБ б) ФСТЭК в) ФСО г) Совет Безопасности РФ
2. Что не относится к основным принципам концепции комплексного обеспечения ИБ? а) Превентивный подход б) Многоуровневая защита в) Централизация управления г) Соблюдение законодательства
3. Какой документ определяет государственную политику в области ИБ? а) Федеральный закон б) Доктрина информационной безопасности в) Указ Президента г) Концепция ИБ
4. Какой метод не используется для выявления уязвимостей в ИС? а) Аудит безопасности б) Тестирование на проникновение в) Анализ рисков г) Резервное копирование
5. Что не относится к организационному обеспечению информационной безопасности? а) Разграничение прав

9. Что из перечисленного не относится к мерам защиты от угрозы нарушения конфиденциальности на уровне организации? а) Разработка политик информационной безопасности б) Обучение персонала вопросам безопасности в) Применение систем контроля доступа г) Использование антивирусного программного обеспечения
10. Какая технология позволяет обеспечить конфиденциальность данных при их хранении на съемных носителях? а) Шифрование съемных носителей б) Контроль целостности в) Использование антивирусного программного обеспечения г) Применение брандмауэров

Тема 6. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа
1. Какая технология используется для обеспечения целостности данных при их передаче по сети? а) Шифрование б) Контроль целостности (хеширование, цифровые подписи) в) Антивирусное программное обеспечение г) Резервное копирование данных
2. Что из перечисленного не является мерой защиты от угрозы нарушения целостности информации? а) Использование RAID-массивов б) Применение систем обнаружения вторжений (IDS/IPS) в) Контроль целостности данных г) Шифрование данных
3. Какая технология позволяет обеспечить целостность данных на уровне хранения? а) Использование RAID-массивов б) Контроль целостности в) Применение антивирусного программного обеспечения г) Резервное копирование данных
4. Что из перечисленного не является мерой защиты от угрозы отказа в обслуживании? а) Использование систем предотвращения вторжений (IPS) б) Применение балансировки нагрузки в) Ограничение сетевого трафика г) Шифрование данных
5. Какая технология используется для обеспечения целостности данных при их хранении на съемных носителях? а) Шифрование съемных носителей б) Контроль целостности данных на съемных носителях в) Использование антивирусного программного обеспечения г) Применение брандмауэров
6. Что из перечисленного не является мерой защиты от угрозы нарушения целостности информации на программном уровне? а) Использование систем обнаружения вторжений (IDS) б) Применение систем контроля целостности в) Шифрование данных г) Обновление программного обеспечения
7. Какая технология позволяет обеспечить целостность данных при их передаче по незащищенным беспроводным сетям? а) Шифрование беспроводной сети (WPA2, WPA3) б) Контроль целостности данных в) Использование антивирусного программного обеспечения г) Применение брандмауэров
8. Что из перечисленного не относится к мерам защиты от угрозы отказа в обслуживании на физическом уровне? а) Использование резервных источников питания б) Применение систем охлаждения в) Ограничение физического доступа в помещения г) Шифрование данных
9. Какая технология позволяет обеспечить целостность данных при их передаче по сети Интернет? а) Использование протокола HTTPS б) Контроль целостности (хеширование, цифровые подписи) в) Применение антивирусного программного обеспечения г) Резервное копирование данных
10. Что из перечисленного не относится к мерам защиты от угрозы нарушения целостности информации на уровне организации? а) Разработка политик информационной безопасности б) Обучение персонала вопросам безопасности в) Применение систем контроля доступа г) Шифрование данных

Тема 7. Политика и модели безопасности
1. Что из перечисленного не относится к основным элементам политики безопасности? а) Цели и задачи политики безопасности б) Область применения политики безопасности в) Техническая документация по реализации политики безопасности г) Стандарты и руководства по обеспечению безопасности
2. Какая модель безопасности основана на принципе "все разрешено, кроме запрещенного"? а) Модель мандатного разграничения доступа б) Модель дискреционного разграничения доступа в) Модель разграничения доступа на основе ролей г) Модель Кларка-Вилсона
4. Что из перечисленного не является основным принципом модели разграничения доступа на основе ролей (RBAC)? а) Пользователи получают разрешения на основе своих ролей б) Роли определяют набор разрешений на доступ к ресурсам в) Каждый пользователь имеет только одну роль г) Разделение обязанностей между ролями
5. Какая модель безопасности основана на принципе "все запрещено, кроме разрешенного"? а) Модель мандатного разграничения доступа б) Модель дискреционного разграничения доступа в) Модель разграничения доступа на основе ролей г) Модель Кларка-Вилсона
6. Что из перечисленного является основным принципом модели Кларка-Вилсона? а) Субъекты и объекты имеют присвоенные уровни секретности б) Субъект может читать и записывать в объекты с равным уровнем секретности в) Целостность данных должна быть обеспечена при их модификации г) Пользователи получают разрешения на основе своих ролей
7. Что из перечисленного не является основным принципом модели Белла-ЛаРадии? а) Субъекты имеют присвоенные уровни секретности б) Объекты имеют присвоенные уровни секретности в) Субъект может читать объекты с равным или меньшим уровнем секретности г) Субъект может записывать в объекты с равным уровнем секретности
8. Что из перечисленного не относится к основным элементам политики безопасности? а) Цели и задачи политики безопасности б) Область применения политики безопасности в) Техническая документация по реализации политики безопасности г) Стандарты и руководства по обеспечению безопасности
9. Какая модель безопасности основана на принципе "наименьших привилегий"? а) Модель мандатного разграничения доступа б) Модель дискреционного разграничения доступа в) Модель разграничения доступа на основе ролей г) Модель Кларка-Вилсона
10. Что из перечисленного не является основным принципом модели Белла-ЛаРадии? а) Субъекты имеют присвоенные уровни секретности б) Объекты имеют присвоенные уровни секретности
в) Субъект может читать объекты с равным или большим уровнем секретности г) Субъект может записывать в объекты с равным или меньшим уровнем секретности

Тема 8. Информационные войны и информационное противоборство

• 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.
• Изучите преимущества и недостатки ролевой модели безопасности.
• Приведите примеры реализации ролевой модели безопасности в информационных системах.
8. Практическая задача:
• Выберите тип информационной системы (например, корпоративная сеть, интернет-магазин, система дистанционного обучения).
• Проанализируйте требования к безопасности этой системы.
• Разработайте политику безопасности для выбранной системы, используя изученные модели разграничения доступа.
• Опишите меры, которые необходимо предпринять для реализации разработанной политики безопасности.

ЗАДАНИЯ К ЛАБОРАТОРНЫМ РАБОТАМ
Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности
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.

 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.
o Разработать рекомендации по устранению выявленных уязвимостей.
• Отчет:
• Описать теоретические основы защиты информации от несанкционированного доступа и нарушения целостности.
• Представить разработанную модель системы защиты информации (вариант 1 или 2).
• Описать результаты анализа уязвимости информационной системы (вариант 3).

6.4. Оценочные средства промежуточной аттестации
ВОПРОСЫ К ЗАЧЕТУ
Знать:
Вопросы на установление последовательности
1. Установите верную последовательность этапов становления теории информационной безопасности:
A. Формирование правовых основ защиты информации
B. Появление первых концепций защиты данных в компьютерных системах
C. Осознание необходимости защиты информации в эпоху цифровизации
D. Разработка комплексных систем защиты информации
2. Установите верную последовательность уровней представления информации как объекта защиты:
A. Семантический уровень (смысл информации)
B. Физический уровень (носители информации)
C. Синтаксический уровень (структура данных)
D. Прагматический уровень (ценность информации для пользователя)
3. Установите верную последовательность шагов разработки государственной политики информационной безопасности:
A. Реализация мер по защите информации
B. Анализ угроз и уязвимостей национальной безопасности
C. Определение приоритетов и целей политики

D. Создание нормативных актов и регулирующих органов
4. Установите верную последовательность действий при анализе угроз информационной безопасности:
A. Классификация выявленных угроз
B. Оценка уязвимостей системы
C. Идентификация потенциальных угроз
D. Разработка мер по снижению рисков
5. Установите верную последовательность принципов построения систем защиты информации:
A. Обеспечение непрерывного мониторинга угроз
B. Определение объектов защиты
C. Применение многоуровневой защиты
D. Анализ рисков и угроз

Вопросы на установление соответствия
1. Установите соответствие между этапами становления теории информационной безопасности и их характеристиками:
1. Разработка первых концепций защиты данных
2. Формирование правовых основ
3. Осознание необходимости защиты информации
4. Создание комплексных систем защиты
A. Появление нормативных актов и законов
B. Развитие компьютерных технологий
C. Рост киберугроз и цифровизация
D. Интеграция многоуровневых подходов
E. Изобретение интернета
2. Установите соответствие между уровнями представления информации и их описаниями:
1. Физический уровень
2. Синтаксический уровень
3. Семантический уровень
4. Прагматический уровень
A. Определяет структуру и формат данных
B. Оценивает ценность информации для пользователя
C. Относится к носителям информации
D. Раскрывает смысл и содержание информации
E. Регулирует доступ к данным
3. Установите соответствие между органами обеспечения информационной безопасности и их задачами:
1. Анализ угроз
2. Реализация мер защиты
3. Разработка нормативных актов
4. Определение приоритетов
A. Установление целей государственной политики
B. Мониторинг уязвимостей и рисков
C. Создание законов и стандартов
D. Внедрение технологий шифрования
E. Обучение персонала
4. Установите соответствие между типами угроз информационной безопасности и их характеристиками:
1. Вирусы
2. Фишинг
3. Взлом системы
4. Утечка данных
A. Несанкционированный доступ к системе
B. Распространение вредоносного кода
C. Передача конфиденциальной информации
D. Обман пользователей для получения данных
E. Физическое уничтожение носителей
5. Установите соответствие между методами защиты информации и их описаниями:
1. Шифрование
2. Аутентификация
3. Контроль доступа
4. Мониторинг угроз
A. Проверка подлинности пользователя
B. Преобразование данных в нечитаемый вид
C. Ограничение прав доступа
D. Постоянное наблюдение за системой
E. Удаление устаревших данных

Уметь:
1. Выберите правильный ответ и обоснуйте свой выбор. Какой этап стал первым в становлении теории информационной безопасности?
A. Формирование правовых основ защиты информации
B. Появление первых концепций защиты данных в компьютерных системах
C. Осознание необходимости защиты информации в эпоху цифровизации

D. Разработка комплексных систем защиты информации
2. Выберите правильный ответ и обоснуйте свой выбор. Какой уровень представления информации определяет ее смысл?
A. Физический уровень
B. Синтаксический уровень
C. Семантический уровень
D. Прагматический уровень
3. Выберите правильный ответ и обоснуйте свой выбор. Что является основной целью государственной политики информационной безопасности?
A. Разработка новых технологий
B. Обеспечение защиты национальных интересов
C. Обучение населения основам кибербезопасности
D. Создание коммерческих систем защиты
4. Выберите правильный ответ и обоснуйте свой выбор. Какая угроза информационной безопасности связана с обманом пользователей?
A. Вирусы
B. Фишинг
C. Взлом системы
D. Утечка данных
5. Выберите правильный ответ и обоснуйте свой выбор. Какой метод защиты информации преобразует данные в нечитаемый вид?
A. Шифрование
B. Аутентификация
C. Контроль доступа
D. Мониторинг угроз
6. Выберите правильный ответ и обоснуйте свой выбор. Что из перечисленного относится к предметной области теории информационной безопасности?
A. Разработка программного обеспечения
B. Анализ уязвимостей и угроз
C. Создание баз данных
D. Маркетинг информационных продуктов
7. Выберите правильный ответ и обоснуйте свой выбор. Какое свойство защищаемой информации связано с ее ценностью для пользователя?
A. Доступность
B. Целостность
C. Конфиденциальность
D. Полезность
8. Выберите правильный ответ и обоснуйте свой выбор. Какой орган занимается созданием нормативных актов в области информационной безопасности?
A. Разработчики систем защиты
B. Государственные регулирующие органы
C. Частные компании
D. Пользователи информационных систем
9. Выберите правильный ответ и обоснуйте свой выбор. Что из перечисленного является первым шагом в анализе угроз?
A. Классификация угроз
B. Оценка уязвимостей
C. Идентификация потенциальных угроз
D. Разработка мер защиты
10. Выберите правильный ответ и обоснуйте свой выбор. Какой принцип построения систем защиты предполагает использование нескольких методов?
A. Многоуровневая защита
B. Непрерывный мониторинг
C. Определение объектов защиты
D. Анализ рисков

Владеть:
1. Прочитайте текст и дайте развернутый ответ: Компания разрабатывает новую систему управления базами данных, которая будет использоваться для хранения и обработки большого объема данных, включая конфиденциальную информацию клиентов. В процессе разработки необходимо учитывать потенциальные угрозы, такие как несанкционированный доступ, утечка данных или их повреждение. Система должна быть спроектирована с учетом современных стандартов безопасности и обеспечивать удобство использования для сотрудников. Также важно предусмотреть возможность масштабирования системы в будущем без ущерба для ее защищенности и соблюдать требования законодательства о защите данных. Как им следует учитывать принципы информационной безопасности на этапе проектирования, чтобы обеспечить конфиденциальность, целостность и доступность данных?
2. Прочитайте текст и дайте развернутый ответ: У организации есть критически важная информация, такая как финансовые данные и коммерческая тайна, которая требует защиты от утечек и атак. Эта информация используется в ключевых бизнес-процессах, и ее компрометация может привести к значительным убыткам. Организация сталкивается с ростом киберугроз, включая внутренние и внешние риски, такие как человеческий фактор и технические уязвимости. Необходимо разработать системный подход, который будет экономически оправданным и не помешает основной деятельности. Каким образом они могут применить концепцию комплексной защиты информации для обеспечения ее безопасности?
3. Прочитайте текст и дайте развернутый ответ: Компания обрабатывает большое количество конфиденциальной информации о клиентах, включая персональные данные, финансовые сведения и историю покупок, которые используются в маркетинге и аналитике. Неправильное обращение с данными может привести к штрафам, ущербу имени и потере доверия

b) Применение методов шифрования данных
c) Анализ угроз нарушения целостности при транспортировке
d) Выбор подходящей технологии защиты
3. Установите верную последовательность этапов проектирования политики безопасности для информационной системы:
a) Реализация субъектно-объектной модели разграничения доступа
b) Определение потребностей в безопасности системы
c) Создание парольной системы разграничения доступа
d) Формулировка аксиом политики безопасности
4. Установите верную последовательность действий для противодействия информационно-психологической войне:
a) Оценка уровня угрозы информационной атаки
b) Использование СМИ для противодействия пропаганде
c) Анализ информационной среды на наличие признаков войны
d) Разработка стратегии информационной защиты
5. Установите верную последовательность применения методов защиты информации на разных уровнях:
a) Применение криптографических методов для защиты конфиденциальности
b) Настройка системы защиты от отказа доступа
c) Реализация ролевой модели безопасности для разграничения доступа
d) Защита целостности данных при обработке

Вопросы на установление соответствия
1. Установите соответствие между методами защиты и их описанием:
1. Идентификация и аутентификация
2. Криптографические методы
3. Инженерно-технические методы
4. Организационные методы
a) Шифрование данных для защиты при передаче
b) Установка физических барьеров и датчиков в помещении
c) Проверка личности пользователя перед предоставлением доступа
d) Разработка внутренних правил и инструкций
e) Анализ содержимого сообщений в социальных сетях
2. Установите соответствие между этапами защиты информации и их характеристиками:
1. Защита при хранении
2. Защита при обработке
3. Защита при транспортировке
4. Защита от отказа доступа
a) Использование контрольных сумм для проверки данных
b) Применение резервных серверов и каналов связи
c) Шифрование данных в канале передачи
d) Ограничение доступа к базам данных
e) Мониторинг активности пользователей в реальном времени
3. Установите соответствие между моделями безопасности и их характеристиками:
1. Дискреционный доступ
2. Мандатный доступ
3. Ролевая модель
4. Субъектно-объектная модель
a) Управление доступом на основе ролей пользователей
b) Разграничение доступа на основе уровней секретности
c) Право владельца ресурса определять доступ
d) Описание взаимодействия между субъектами и объектами
e) Использование биометрических данных для входа
4. Установите соответствие между видами информационных войн и их целями:
1. Информационно-техническая война
2. Информационно-психологическая война
3. Информационное противоборство
4. Использование СМИ
a) Формирование общественного мнения
b) Нарушение работы информационных систем
c) Противодействие пропаганде противника
d) Влияние на психику и поведение людей
e) Разработка новых программных продуктов
5. Установите соответствие между методами защиты и уровнем их применения:
1. Криптографические методы
2. Парольные системы
3. Защита целостности при транспортировке
4. Политика безопасности
a) Разграничение доступа на уровне пользователей
b) Защита данных при передаче по сети
c) Обеспечение конфиденциальности информации
d) Установление правил для всей системы

e) Физическая защита серверных помещений

Уметь:
1. Выберите правильный ответ и обоснуйте свой выбор: Что является основным способом предотвращения несанкционированного доступа (НСД)?
a) Установка антивирусного ПО
b) Идентификация и аутентификация пользователей
c) Шифрование данных
d) Ограничение физического доступа
2. Выберите правильный ответ и обоснуйте свой выбор: Какой метод защиты наиболее эффективен против утечки по техническим каналам?
a) Установка межсетевых экранов
b) Использование криптографии
c) Регулярное обновление ПО
d) Обучение персонала
3. Выберите правильный ответ и обоснуйте свой выбор: Что обеспечивает защиту целостности информации при хранении?
a) Резервное копирование
b) Контрольные суммы
c) Шифрование
d) Многофакторная аутентификация
4. Выберите правильный ответ и обоснуйте свой выбор: Какой метод лучше всего защищает от угрозы отказа доступа?
a) Использование цифровых подписей
b) Резервирование серверов
c) Ограничение прав доступа
d) Мониторинг сети
5. Выберите правильный ответ и обоснуйте свой выбор: Какая модель разграничения доступа основана на уровнях секретности?
a) Дискреционная модель
b) Мандатная модель
c) Ролевая модель
d) Тематическая модель
6. Выберите правильный ответ и обоснуйте свой выбор: Что является ключевым элементом политики безопасности?
a) Установка антивирусов
b) Формулировка аксиом безопасности
c) Обновление оборудования
d) Проведение аудита
7. Выберите правильный ответ и обоснуйте свой выбор: Какой подход лучше всего подходит для управления доступом в крупной организации?
a) Парольные системы
b) Дискреционный доступ
c) Ролевая модель
d) Мандатный доступ
8. Выберите правильный ответ и обоснуйте свой выбор: Что является основной целью информационно-психологической войны?
a) Уничтожение серверов
b) Влияние на поведение людей
c) Перехват данных
d) Разработка вирусов
9. Выберите правильный ответ и обоснуйте свой выбор: Какой метод наиболее эффективен для противодействия пропаганде?
a) Использование СМИ
b) Блокировка интернета
c) Шифрование сообщений
d) Физическая защита объектов
10. Выберите правильный ответ и обоснуйте свой выбор: Какой метод защиты одновременно обеспечивает конфиденциальность и целостность данных?
a) Многофакторная аутентификация
b) Цифровая подпись
c) Резервирование данных
d) Физическая защита серверов

Владеть:
1. Прочитайте текст и дайте развернутый ответ: Компания обрабатывает большое количество конфиденциальной информации о клиентах. Эта информация включает персональные данные, такие как имена, адреса, номера телефонов и финансовые сведения. Сотрудники работают с данными через внутреннюю сеть, которая подключена к интернету. Недавно в компании зафиксировали попытки внешнего вмешательства в систему. Руководство обеспокоено возможными утечками и штрафами за нарушение законодательства о защите данных. Для предотвращения подобных инцидентов необходимо внедрить комплексные меры безопасности. Какие меры по защите от несанкционированного доступа следует предпринять?
2. Прочитайте текст и дайте развернутый ответ: В организации обнаружена утечка данных через технический канал. Утечка произошла из-за перехвата электромагнитных сигналов от оборудования в серверной комнате. Это позволило злоумышленникам получить доступ к конфиденциальной информации. Сотрудники не были осведомлены о таких рисках, а

3. Что входит в предметную область теории информационной безопасности? a) Разработка вредоносного ПО b) Создание технических средств защиты информации c) Управление информационными рисками d) Все вышеперечисленное
4. Какое из перечисленных свойств защищаемой информации считается наиболее важным? a) Целостность b) Конфиденциальность c) Доступность d) Все свойства равнозначны
5. Какие уровни представления информации существуют? a) Физический и логический b) Внутренний и внешний c) Синтаксический, семантический и прагматический d) Цифровой и аналоговый
6. 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
7. Какой орган отвечает за контрразведывательную деятельность в области обеспечения информационной безопасности? a) ФСБ России b) ФСТЭК России
c) Минцифры России d) Роскомнадзор
8. 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
9. 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"
10. 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
11. Какие существуют основные направления реализации угроз информационной безопасности? a) Физические, технические, программные b) Внешние, внутренние, комбинированные c) Инсайдерские, хакерские, хактивистские d) Преднамеренные, случайные, стихийные
12. Что такое анализ уязвимостей системы? a) Выявление и устранение недостатков в системе защиты информации b) Классификация угроз информационной безопасности c) Оценка эффективности мер защиты информации
d) Разработка новых методов защиты информации
13. Какие методы и инструменты используются для проведения анализа уязвимостей? a) Сканеры уязвимостей, системы обнаружения вторжений b) Антивирусные программы, брандмауэры c) Средства шифрования, системы аутентификации d) Программы резервного копирования, RAID-массивы
14. Какая из перечисленных угроз относится к нарушению целостности информации? a) Кража данных b) DoS-атака
c) Вредоносное ПО d) Инсайдерская угроза
15. Какая из перечисленных угроз относится к нарушению доступности информации? a) Фишинг b) DDoS-атака c) Вирус-вымогатель d) Кейлоггер

ТЕСТОВЫЕ ЗАДАНИЯ К ЭКЗАМЕНУ

1. Какой метод используется для предотвращения несанкционированного доступа?
a) Криптографический
b) Организационный
c) Инженерно-технический
d) Все вышеперечисленные
2. Что такое идентификация?
a) Процесс присвоения объекту уникального идентификатора
b) Процесс проверки принадлежности объекта конкретному субъекту
c) Процесс разграничения прав доступа
d) Процесс шифрования данных
3. Какой метод используется для защиты информации на уровне содержания?
a) Криптографический
b) Стеганографический
c) Кодирование
d) Компрессия
4. Какой метод применяется для защиты целостности информации при хранении?
a) Электронная цифровая подпись
b) Контрольные суммы
c) Шифрование данных
d) Все вышеперечисленные
5. Какая угроза связана с нарушением целостности информации?
a) Потеря данных
b) Несанкционированное изменение данных
c) Утечка данных
d) Отказ в обслуживании
6. Что является основной целью системы защиты от отказа доступа?
a) Предотвращение несанкционированного доступа
b) Обеспечение доступности информации для авторизованных пользователей
c) Защита целостности данных
d) Защита конфиденциальности данных
7. Что такое субъектно-объектная модель разграничения доступа?
a) Модель, в которой субъекты взаимодействуют с объектами в соответствии с определенными правилами
b) Модель, основанная на паролях
c) Модель, в которой доступ определяется ролями пользователей
d) Модель, основанная на категориях безопасности

b) Манипулирование общественным мнением и распространение пропаганды
c) Кибератаки на информационные системы
d) Сбор разведывательных данных
12. Какие средства используются в информационных войнах?
a) Информационные технологии
b) Средства массовой информации
c) Кибероружие
d) Все вышеперечисленные
13. Что является одной из целей противодействия информационным войнам?
a) Обеспечение информационной безопасности
b) Нанесение ущерба инфраструктуре противника
c) Распространение пропаганды
d) Кибератаки на информационные системы
14. Какие навыки необходимы для противодействия информационным войнам?
a) Управление информационными ресурсами и контентом
b) Проведение кибератак
c) Распространение дезинформации
d) Нет правильного ответа
15. Какая угроза связана с информационными войнами?
a) Потеря данных
b) Несанкционированное изменение данных
c) Манипулирование общественным мнением
d) Отказ в обслуживании

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	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.1.2	О.В. Прохорова Информационная безопасность и защита информации:учебник. - СПб.: Лань, 2023. - 124 с.: ил.
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
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	ПЛАТФОРМА ОНЛАЙН-ОБРАЗОВАНИЯ «РАЗУМ». Режим доступа: https://razoom.mgutm.ru/
7.3.5	Сайт национального открытого университета "ИНТУИТ". Режим доступа: https://intuit.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. № __
И.о.зав. кафедрой Левчук Валерия Владимировна _____

Рабочая программа согласована на заседании выпускающей кафедры
Физика, математика и информационные технологии
Протокол от __ _____ 2027 г. № __
И.о.зав. кафедрой Левчук Валерия Владимировна _____

==========

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. № __
И.о.зав. кафедрой Левчук Валерия Владимировна _____

Рабочая программа согласована на заседании выпускающей кафедры
Физика, математика и информационные технологии
Протокол от __ _____ 2028 г. № __
И.о.зав. кафедрой Левчук Валерия Владимировна _____

==========

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. № __
И.о.зав. кафедрой Левчук Валерия Владимировна _____

Рабочая программа согласована на заседании выпускающей кафедры
Физика, математика и информационные технологии
Протокол от __ _____ 2029 г. № __
И.о.зав. кафедрой Левчук Валерия Владимировна _____

==========

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. № __
И.о.зав. кафедрой Левчук Валерия Владимировна _____

Рабочая программа согласована на заседании выпускающей кафедры
Физика, математика и информационные технологии
Протокол от __ _____ 2030 г. № __
И.о.зав. кафедрой Левчук Валерия Владимировна _____