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)»

УТВЕРЖДАЮ
И.о. директора ДКГИПТиБ (филиала)
Г.В. Павлятенко
23 апреля 2024 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
Общая трудоемкость:	216 часов/6 з.е.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00AA7853CEFA35F0837BA866654F3503A6
Владелец: Павлятенко Геннадий Владимирович
Действителен: с 08.12.2025 до 03.03.2027

Ростов-на-Дону, 2024 г.

Программу составил(и):
ст. преподаватель Ковалев Д.В.

Рабочая программа дисциплины (модуля)
"Информационная безопасность"
разработана составлена на основании учебного плана, утвержденного ученым советом 28 марта 2024 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
доц., канд. экон. наук, доц. Мурат Е.П._____ _____

Рабочая программа обсуждена на заседании обеспечивающей кафедры
Физика, математика и информационные технологии
Протокол от 23 апреля 2024 г. № 8
И.о. зав. кафедрой Мурат Елена Петровна _____

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С РЕЗУЛЬТАТАМИ ОСВОЕНИЯ 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

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цели:

Цель учебной дисциплины заключается в получении обучающимися теоретических знаний и практических навыков в области информационной безопасности

1.2. Задачи:

1. изложение теоретических основ информационной безопасности;
2. изучение нормативно-правовой базы в области информационной безопасности в РФ, включая нормативно-правовое регулирование защиты персональных данных;
3. ознакомление с современными криптографическими алгоритмами и возможностями технической защиты информации;
4. приобретение навыков работы по обеспечению пользовательской безопасности и безопасности персональных данных.

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

Цикл (раздел) ОП: Б1.О

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 2/6			
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			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 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	Часов	Интеракт.	Прак. подг.	Индикаторы достижения компетенции	Оценочные средства
	Раздел 1.История и современные методы криптографической защиты информации						
1.1	**История и современные методы криптографической защиты информации Краткое содержание: Понятия криптологии, криптографии, крипто анализа, ключ шифра. Первые шифры замены и перестановки (шифр сциталя, шифр цезаря). Шифр Виженера. Решетка Кардано. Стенографические методы защиты информации. Становление математических и технических основ защиты информации в Новое время. Начало формирования научных приёмов защиты информации. Изобретение электромагнитного телеграфа и первых механических шифр машин. Семейство машин Энигма. Крипто анализ шифра Энигма. Изобретение совершенно секретного шифра («одноразовый шифр блокнот»), преимущества и проблемы его использования. Понятие криптографического протокола. Ключи. Симметричные методы шифрования (шифрование с закрытым ключом): технологии, стойкость, преимущества и недостатки. Асимметричные методы шифрования (шифрование с открытым ключом): технологии, стойкость, преимущества и недостатки. Атака "человек посередине". Цифровая подпись. Сертификаты и УЦ Предполагаемые результаты обучения: ЗНАТЬ основы криптографической защиты информации (симметричное и ассиметричное шифрование, хэш-функции, электронная подпись) /Лек/**	6	4	0	0	ОПК-3.1	устный опрос
1.2	**Криптографические и стеганографические методы защиты информации Краткое содержание: Сравнение данных с помощью хэш-функции. Важно понимать, были ли данные повреждены или была совершена попытка их фальсификации. Для определения того, были ли данные изменены или остались такими же, можно использовать программу хэширования. Программа хэширования выполняет преобразование данных или файла используя хэш-функцию, которая**	6	2	0	1	ОПК-3.2,ОПК-3.3	отчет о практической работе

	выдает некое значение (обычно значительно короче, чем сами исходные данные). Существует множество разных хэш-функций, одни очень простые, другие, напротив, очень сложные. Если одна и та же хэш-функция выполняется для преобразования одних и тех же данных, то значение, которое будет получено, будет всегда одинаково. Если данные были каким-то образом изменены, то полученное значение хэш **Предполагаемые результаты обучения:** **УМЕТЬ: применять основные криптографические методы для защиты информации, включая использование симметричных и асимметричных алгоритмов шифрования** **ВЛАДЕТЬ: навыками выбора криптографических методов в зависимости от конкретных задач защиты информации** **/Пр/**						
1.3	**Стеганографические методы защиты информации** **Краткое содержание: Необходимо знакомиться с теоретическим материалом. Произвести установку программного продукта Masker; спрятать текстовый файл в изображении, выбрав алгоритм шифрования пароля; отправить зашифрованное сообщение по электронной почте; извлечь текстовый файл из изображения; удалить извлечённый текстовый файл, без возможности для восстановления.** **Предполагаемые результаты обучения:** **УМЕТЬ: применять основные стеганографические методы для защиты информации, а также уметь к внедрять и извлекать скрытую информацию с использованием стеганографических техник.** **ВЛАДЕТЬ: навыками выбора стеганографических методов в зависимости от конкретных задач защиты информации.** **/Пр/**	6	2	0	1	ОПК-3.2,ОПК-3.3	отчет о практической работе
1.4	**Подготовка реферата по индивидуальной теме** **Краткое содержание: Составление реферата по индивидуальной теме по информационной безопасности. Отбор актуальной исследовательской практики в области ИБ, анализ и сравнение различных методов и моделей. Определение роли информационной безопасности в современном цифровом мире и предложение рекомендаций для**	6	64	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы для самоподготовки

	повышения безопасности информационных систем. Предполагаемые результаты обучения: ЗНАТЬ основы криптографической защиты информации (симметричное и ассиметричное шифрование, хэш-функции, электронная подпись) УМЕТЬ: применять основные криптографические методы для защиты информации, включая использование симметричных и асимметричных алгоритмов шифрования, : применять основные стеганографические методы для защиты информации, а также уметь к внедрять и извлекать скрытую информацию с использованием стеганографических техник ВЛАДЕТЬ: навыками выбора криптографических методов в зависимости от конкретных задач защиты информации, навыками выбора стеганографических методов в зависимости от конкретных задач защиты информации /Ср/						
	Раздел 2.Нормативно-правовое регулирование информационной безопасности в РФ						
2.1	**Нормативно-правовое регулирование информационной безопасности в РФ Краткое содержание: Государственная тайна, коммерческая тайна. Истоки правового регулирования персональных данных в России и за рубежом. Всеобщая декларации прав человека, Конвенция ООН «О защите физических лиц при автоматизированной обработке персональных данных», ФЗ № 152 «О персональных данных». Понятие персональных данных (ФЗ № 152). Основные определения ФЗ № 152. Виды персональных данных. Общие (общедоступные), биометрические, специальные и иные персональные данные. Обезличенные персональные данные. Обратимое и необратимое обезличивание. Информационная система персональных данных (ИСПДн). Состав ИСПДн. Требования к оператору персональных данных. Уровни защищенности ИСПДн. Типы актуальных угроз (1,2, 3 типы). Порядок определения актуальных угроз безопасности персональных данных в информационных системах персональных данных. Показатели исходной защищенности ИСПДн (по**	7	4	0	0	ОПК-3.1	устный опрос

	территориальному размещению, по наличию соединения с сетями общего пользования, по встроенным (легальным) операциям с записями баз персональных данных, по разграничению доступа к персональным данным, по наличию соединений с другими базами ПДн иных ИСПДн, по уровню обобщения (обезличивания) ПДн, по объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки).Регистрация оператора в Роскомнадзоре. Согласие на обработку персональных данных. Обработка ПДн в «облаке». Ответственность за разглашение персональных данных. Предполагаемые результаты обучения: ЗНАТЬ терминологические основы информационной безопасности, составляющие информационной безопасности, нормативно-правовую базу регулирования информации и защиты информации /Лек/						
2.2	**Организация защиты персональных данных Краткое содержание: Определение перечня угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Определение уровня исходной защищённости. Определение частоты (вероятности) реализации рассматриваемой угрозы. Определение коэффициента реализуемости угрозы (Y) и возможности реализации. Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Определение типа актуальной угрозы. Определение уровня защищенности ПДН. Определение состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах ПДН. Предполагаемые результаты обучения: УМЕТЬ: формулировать базовые определения в области информационной безопасности, выбирать и использовать современные информационно-коммуникационные средства в области информационной**	7	4	0	0	ОПК-3.2,ОПК-3.3	отчет о практической работе

	безопасности для обеспечения безопасности персональных данных в организации, определять уровень исходной защищенности информационных систем персональных данных ВЛАДЕТЬ: навыками определения стратегии работы с персональными данными в организации /Пр/						
2.3	**Терминологические основы информационной безопасности Краткое содержание: . В сети Интернет найдите определения нижеперечисленным терминам, обращая внимание на степень достоверности источника (возможно указать несколько разных определений для одного и того же термина). Для каждого определения необходимо обозначить источник. Предполагаемые результаты обучения: ЗНАТЬ терминологические основы информационной безопасности, составляющие информационной безопасности, нормативно-правовую базу регулирования информации и защиты информации УМЕТЬ: формулировать базовые определения в области информационной безопасности, выбирать и использовать современные информационно-коммуникационные средства в области информационной безопасности для обеспечения безопасности персональных данных в организации, определять уровень исходной защищенности информационных систем персональных данных ВЛАДЕТЬ: навыками определения стратегии работы с персональными данными в организации /Ср/**	7	42	0	0	ОПК-3.1,ОПК-3.2	вопросы для самоподготовки
	Раздел 3.Информационная безопасность пользователя						
3.1	**Информационная безопасность пользователя Краткое содержание: Фишинг. Основные варианты фишинга. Способы фишинга. Тайпсвотинг. Троянский конь. Квид про Кво. Претекстинг. «Дорожное яблоко». Сбор информации из открытых источников. Обратная социальная инженерия. Вредоносное ПО. Способы защиты информации от вредоносного ПО. Стойкость паролей. Предполагаемые результаты обучения: ЗНАТЬ современные программно-**	7	4	0	0	ОПК-3.1	устный опрос

	технические средства защиты данных для решения задач профессиональной деятельности, основные угрозы информационной безопасности, современные виды компьютерных преступлений /Лек/						
3.2	**Блокирование рекламы и нежелательных объектов на веб-страницах Краткое содержание: Блокирование рекламы и нежелательных объектов на веб-страницах с помощью утилиты Adguard. Предполагаемые результаты обучения: УМЕТЬ использовать современные информационно-коммуникационные средства блокирования рекламы и нежелательных объектов на веб-страницах ВЛАДЕТЬ: навыками выбора наилучших методов блокирования рекламы и нежелательных объектов на веб-страницах /Лаб/**	7	2	0	0	ОПК-3.2,ОПК-3.3	отчет о лабораторной работе
3.3	**Установка и настройка расширения для браузера Краткое содержание Установка и настройка расширения для браузера AdblockPlus. Блокирование загрузки и показа различных элементов страницы Предполагаемые результаты обучения: УМЕТЬ использовать современные информационно-коммуникационные средства блокирования загрузки и показа различных элементов страницы ВЛАДЕТЬ: навыками выбора наилучших методов блокирования загрузки и показа различных элементов страницы /Лаб/**	7	6	0	0	ОПК-3.2,ОПК-3.3	отчет о лабораторной работе
3.4	**Антивирусное программное обеспечение Краткое содержание: Рассмотреть средства защиты, интегрированные в Kaspersky End Point Security и настроить приложение Предполагаемые результаты обучения: УМЕТЬ использовать современные информационно-коммуникационные средства антивирусной защиты ВЛАДЕТЬ: навыками выбора наилучших методов антивирусной защиты /Пр/**	7	4	0	0	ОПК-3.2,ОПК-3.3	отчет о практической работе
3.5	**Информационная безопасность пользователя Самостоятельная работа по теме**	7	42	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы для самоподготовки

	"Информационная безопасность пользователя" включает в себя изучение основных принципов и методов обеспечения безопасности в цифровой среде, анализ современных угроз, и разработку индивидуальных стратегий защиты личных данных. Предполагаемые результаты обучения: ЗНАТЬ современные программно-технические средства защиты данных для решения задач профессиональной деятельности, основные угрозы информационной безопасности, современные виды компьютерных преступлений УМЕТЬ формулировать и соблюдать необходимые правила "цифровой гигиены", выбирать и использовать современные информационно-коммуникационные средства в области информационной безопасности для обеспечения личной информационной безопасности ВЛАДЕТЬ: навыками определения необходимых методов и средств защиты информации в зависимости от конкретных задач пользователя /Ср/						
	Раздел 4.Промежуточный контроль						
4.1	**Промежуточный контроль (зачет) Предполагаемые результаты обучения: ЗНАТЬ современные программно-технические средства защиты данных для решения задач профессиональной деятельности, терминологические основы информационной безопасности, составляющие информационной безопасности, нормативно-правовую базу регулирования информации и защиты информации, основы криптографической защиты информации (симметричное и ассиметричное шифрование, хэш-функции, электронная подпись) УМЕТЬ формулировать базовые определения в области информационной безопасности, формулировать и соблюдать необходимые правила "цифровой гигиены", выбирать и использовать современные информационно-коммуникационные средства в области информационной безопасности для обеспечения безопасности персональных данных в организации, определять уровень исходной защищенности информационных систем персональных данных**	6	0	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы к зачету, итоговое тестирование

	ВЛАДЕТЬ навыками определения стратегии работы с персональными данными в организации /Зачёт/						
4.2	**Промежуточный контроль (экзамен) Результаты обучения: 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 /Экзамен/**	7	36	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы к экзамену, итоговое 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 педагогического работника, отнесенного к профессорско-преподавательскому составу (далее – преподаватель) и (или) лиц, привлекаемых к реализации образовательных программ на иных условиях, но без их непосредственного участия.
СРС по заданию и при методическом руководстве преподавателя и (или) лиц, привлекаемых к реализации 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, НИР, 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 этапов формирования индикаторов их достижения в процессе освоения ОПОП

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 информационной и библиографической культуры, методов и средств решения стандартных задач профессиональной деятельности 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

Владеет отдельными навыками подготовки обзоров, аннотаций, составления рефератов с учетом требований информационной безопасности

Пороговый уровень:

Сформированы базовые структуры знаний принципов информационной и библиографической культуры, методов и средств решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности фрагментарно и носит репродуктивный характер

Владеет навыками подготовки обзоров, аннотаций, составления рефератов с учетом требований информационной безопасности

Продвинутый уровень:

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

Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности применяется в решении типовых заданий

Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций с учетом требований информационной безопасности

Высокий уровень:

Знания принципов информационной и библиографической культуры, методов и средств решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности твердые, аргументированные и всесторонние

Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности успешно применяется в решении как типовых, так и нестандартных творческих заданий

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

6.2. Шкала оценивания в зависимости от уровня сформированности компетенций

Уровень сформированности компетенций

Характеристики индикаторов достижения компетенций	**1. Недостаточный: компетенции не сформированы.**	**2. Пороговый: компетенции сформированы.**	**3. Продвинутый: компетенции сформированы.**	**4. Высокий: компетенции сформированы.**
Знания:	Знания отсутствуют.	Сформированы базовые структуры знаний.	Знания обширные, системные.	Знания твердые, аргументированные, всесторонние.
Умения:	Умения не сформированы.	Умения фрагментарны и носят репродуктивный характер.	Умения носят репродуктивный характер применяются к решению типовых заданий.	Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий.
Навыки:	Навыки не сформированы.	Демонстрируется низкий уровень самостоятельности практического навыка.	Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка.

Описание критериев оценивания

Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала;	Обучающийся демонстрирует: - знания теоретического материала;	Обучающийся демонстрирует: - знание и понимание основных вопросов	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания

- допускаются 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; - отсутствие готовности (способности) к дискуссии и низкая степень контактности.	- 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; - умение без грубых ошибок решать практические задания, которые следует выполнить.	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; - наличие собственной обоснованной позиции по обсуждаемым вопросам. Возможны незначительные оговорки и неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.	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»**

Оценочные средства, обеспечивающие диагностику сформированности компетенций, заявленных в рабочей программе по дисциплине (молулю) для проведения промежуточной аттестации

ОЦЕНИВАНИЕ УРОВНЯ ЗНАНИЙ: Теоретический блок вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и излагать материал.
1. Недостаточный уровень
Знания принципов информационной и библиографической культуры, методов и средств решения стандартных задач профессиональной деятельности 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
Владеет отдельными навыками подготовки обзоров, аннотаций, составления рефератов с учетом требований информационной безопасности
2. Пороговый уровень
Сформированы базовые структуры знаний принципов информационной и библиографической культуры, методов и средств решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности фрагментарно и носит репродуктивный характер
Владеет навыками подготовки обзоров, аннотаций, составления рефератов с учетом требований информационной безопасности
3. Продвинутый уровень
Знания принципов информационной и библиографической культуры, методов и средств решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности обширные и системные
Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности применяется в решении типовых заданий
Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций с учетом требований информационной безопасности
4. Высокий уровень
Знания принципов информационной и библиографической культуры, методов и средств решения стандартных задач

профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности твердые, аргументированные и всесторонние
Умение решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности успешно применяется в решении как типовых, так и нестандартных творческих заданий
Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

6.3. Оценочные средства текущего контроля (примерные темы докладов, рефератов, эссе)

Вопросы для устного опроса.

Тема 1. История и современные методы криптографической защиты информации

Какие основные принципы лежат в основе исторических методов криптографии?
Какую роль сыграли криптографические методы в военных и политических событиях прошлого?
Какие были первые применяемые криптографические методы в истории?
Каким образом шифр Цезаря обеспечивал конфиденциальность сообщений?
Как развивалась криптография в средние века?
Какие криптографические системы использовались в эпоху Ренессанса?
Каковы основные принципы шифрования в эпоху кодов и шифровальных машин?
Какие технологические изменения повлияли на современные методы криптографии?
Какова роль математики в современной криптографии?
Какие современные алгоритмы криптографии симметричного ключа вы знаете?
Как работают асимметричные алгоритмы криптографии, такие как RSA?
Что такое хеш-функции и как они используются в криптографии?
Какие методы обеспечивают аутентификацию в современных системах криптографии?
Какие вызовы представляют современные тенденции в области криптографии?
Как криптография влияет на обеспечение кибербезопасности в наше время?

Тема 2. Нормативно-правовое регулирование информационной безопасности в РФ

Какова роль нормативно-правового регулирования в обеспечении информационной безопасности в России?
Какие основные законы и нормативные акты регулируют информационную безопасность в РФ?
Какие ответственности предусмотрены для юридических лиц в области информационной безопасности согласно действующему законодательству?
Какие меры по защите персональных данных установлены законодательством РФ?
Каковы основные требования к организации и проведению аудита информационной безопасности согласно российскому законодательству?
Какие санкции предусмотрены за нарушение законодательства в области информационной безопасности?
Как регулируется вопрос об обязательной сертификации средств защиты информации в России?
Какие нормы касаются обеспечения критической информационной инфраструктуры в стране?
Каким образом государство регулирует использование криптографических средств и технологий в РФ?
Какие требования предъявляются к организациям в сфере телекоммуникаций в контексте обеспечения информационной безопасности?
Какова роль Федеральной службы по техническому и экспортному контролю в области информационной безопасности?
Какие нормы регулируют вопросы кибербезопасности и борьбы с киберпреступностью в России?
Как государство поддерживает развитие отечественных средств защиты информации?
Какие изменения в нормативно-правовой базе РФ связаны с актуальными вызовами в области информационной безопасности?
Как обеспечивается координация между различными органами и ведомствами в рамках регулирования информационной безопасности в России?

Тема 3. Информационная безопасность пользователя

Какие основные угрозы информационной безопасности могут возникнуть для обычного пользователя?
Каковы основные принципы безопасного использования паролей?
Какие меры безопасности следует предпринимать при использовании общественных Wi-Fi сетей?
Как защитить свой компьютер от вредоносных программ, таких как вирусы и трояны?
Какова роль антивирусных программ в обеспечении информационной безопасности пользователя?
Как избежать фишинговых атак при работе в интернете?
Как важно обновлять программное обеспечение для обеспечения безопасности?
Какие меры безопасности применяются при онлайн-платежах и интернет-банкинге?
Каковы рекомендации по сохранению и безопасному обмену конфиденциальной информацией?
Какие риски связаны с использованием облачных сервисов, и как обеспечить их безопасность?
Как избежать социальной инженерии и защитить свою личную информацию?
Каковы основные принципы безопасного использования мобильных устройств?
Как обеспечить безопасность своей электронной почты от вредоносных атак?
Какова важность регулярного резервного копирования данных для пользователя?
Как правильно управлять настройками конфиденциальности в социальных сетях?

Вопросы для самоподготовки.

Тема 1. История и современные методы криптографической защиты информации

Какие криптографические методы использовались в древности для защиты информации?
Какую роль криптография играла в исторических событиях и военных конфликтах?

Какие изменения принесла с собой эпоха Ренессанса в развитие криптографии?
Какие применялись методы криптографии в эпоху кодов и шифровальных машин?
Какие ключевые аспекты современной криптографии отличают ее от исторических методов?
Как работают алгоритмы криптографии симметричного ключа?
Как алгоритмы криптографии симметричного ключа обеспечивают конфиденциальность данных?
Какую роль играет математика в разработке современных криптографических алгоритмов?
Что представляют собой асимметричные алгоритмы криптографии и чем они отличаются от симметричных?
Что такое хеш-функции и как они применяются в современной криптографии?
Какие методы обеспечивают целостность данных в контексте криптографии?
Какие вызовы стоят перед современными системами криптографии в свете технологического развития?
Какие перспективы развития криптографии вы видите в контексте современных вызовов в области информационной безопасности?

Тема 2. Нормативно-правовое регулирование информационной безопасности в РФ
Какие законы Российской Федерации регулируют информационную безопасность?
Какие меры по защите персональных данных установлены в законодательстве?
Какие обязанности по обеспечению информационной безопасности возлагаются на юридические лица?
Что предусмотрено законодательством о кибербезопасности в России?
Какие санкции могут быть применены за нарушение законов в области информационной безопасности?
Как организуется и проводится аудит информационной безопасности согласно российскому законодательству?
Какова роль Федеральной службы по техническому и экспортному контролю в области информационной безопасности?
Как регулируется использование криптографии в России?
Какие требования предъявляются к средствам защиты информации?
Какие нормы регулируют обеспечение критической информационной инфраструктуры?
Как государство поддерживает развитие отечественных средств защиты информации?
Какие изменения в нормативно-правовой базе связаны с вызовами современной информационной среды?
Какие требования предъявляются к организациям в сфере телекоммуникаций в контексте информационной безопасности?
Как органы власти сотрудничают для обеспечения информационной безопасности?
Какие перспективы и изменения можно ожидать в нормативно-правовой области информационной безопасности в ближайшие годы?

Тема 3. Информационная безопасность пользователя
Какие шаги вы предпринимаете для обеспечения безопасности своего пароля?
Какие виды мошенничества вы знаете в онлайн-среде, и как избегаете их?
Как обновляете программное обеспечение на своем устройстве для поддержания безопасности?
Каковы основные принципы безопасного использования общественных Wi-Fi сетей?
Какие меры предосторожности вы принимаете при работе с электронной почтой?
Как избегаете фишинговых атак при использовании интернета?
Какие меры безопасности вы применяете при онлайн-платежах или интернет-банкинге?
Как обеспечиваете безопасность своего компьютера от вредоносных программ?
Как управляете конфиденциальностью в социальных сетях?
Как обеспечиваете безопасность своего мобильного устройства?
Как реагируете на подозрительные сообщения или запросы в интернете?
Какие практики безопасности вы применяете при использовании облачных сервисов?
Какие меры предпринимаете для защиты личной информации от социальной инженерии?
Как сохраняете и регулярно обновляете резервные копии важных данных?
Как обеспечиваете безопасность своей домашней беспроводной сети?

Темы лабораторных и практических работ.
Тема 1. История и современные методы криптографической защиты информации
Практическая работа 1.1. Сравнение данных с помощью хэш-функции
Практическая работа 1.2 . Стеганографические методы защиты информации

Тема 2. Нормативно-правовое регулирование информационной безопасности в РФ
Практическая работа 2.1. Организация защиты персональных данных

Тема 3. Информационная безопасность пользователя
Лабораторная работа 3.1. Блокирование рекламы и нежелательных объектов на веб-страницах с помощью утилиты Adguard.
Лабораторная работа 3.2. Установка и настройка расширения для браузера AdblockPlus.
Лабораторная работа 3.3. Антивирусное программное обеспечение

6.4. Оценочные средства промежуточной аттестации.
Вопросы к зачету:
Вопросы для проверки уровня обученности «знать»
1. Назовите основные принципы информационной безопасности.
2. Дайте определение термину "криптография" и ее роль в обеспечении информационной безопасности.
3. Перечислите основные виды угроз информационной безопасности.
4. Назовите методы защиты от социальной инженерии.

5. Дайте определение термину "фишинг" и объясните, как предотвращать такие атаки.
6. Перечислите основные шаги для создания надежного пароля.
7. Назовите основные методы борьбы с вредоносным программным обеспечением.
8. Дайте определение термину "бэкап" и почему это важный аспект информационной безопасности.
9. Перечислите основные принципы безопасной работы с электронной почтой.
10. Назовите методы защиты от атаки типа "отказ в обслуживании" (DDoS).
11. Дайте определение термину "блокчейн" и расскажите, как он может использоваться в обеспечении безопасности данных.
12. Перечислите основные этапы аудита информационной безопасности.
13. Назовите основные требования к защите мобильных устройств от угроз безопасности.
14. Дайте определение термину "биометрия" и объясните, как она используется в системах аутентификации.
15. Перечислите основные меры по обеспечению физической безопасности информационной инфраструктуры.

Вопросы для проверки уровня обученности «уметь»
1. Охарактеризуйте основные принципы защиты информационной безопасности.
2. Сформулируйте методы предотвращения атаки типа "фишинг".
3. Дайте характеристику средствам многофакторной аутентификации.
4. Охарактеризуйте процедуру создания безопасного пароля и принцип его использования.
5. Сформулируйте меры по защите от вредоносного программного обеспечения.
6. Дайте характеристику термину "криптография" и ее роль в обеспечении безопасности информации.
7. Охарактеризуйте основные этапы аудита информационной безопасности.
8. Сформулируйте методы защиты от атаки "отказ в обслуживании" (DDoS).
9. Дайте характеристику системам обнаружения вторжений и их роль в обеспечении безопасности.
10. Охарактеризуйте требования к защите мобильных устройств от угроз безопасности.
11. Сформулируйте меры по обеспечению безопасности работы с электронной почтой.
12. Дайте характеристику термину "блокчейн" и его роль в обеспечении безопасности данных.
13. Охарактеризуйте принципы физической безопасности информационной инфраструктуры.
14. Сформулируйте методы защиты от социальной инженерии.
15. Дайте характеристику биометрическим технологиям в системах аутентификации.

Вопросы для проверки уровня обученности «владеть»

1. Разработайте политику, включающую основные виды угроз информационной безопасности для организации в современном цифровом мире.
2. Разработайте и предложите реализацию политики паролей, удовлетворяющей современным стандартам безопасности.
3. Предложите методы и обучающие программы для сотрудников по распознаванию и предотвращению атак методом фишинга.
4. Проанализируйте и сравните различные инструменты мониторинга безопасности сети и выберите наилучший для организации.
5. Разработайте план действий при обнаружении инцидента безопасности, включая процедуры изоляции и восстановления.
6. Составьте план проведения аудита безопасности информационной системы, включая выбор методологии и инструментов.
7. Проанализируйте существующие системы DLP (Data Loss Prevention) и предложите реализацию в организации.
8. Проведите анализ безопасности веб-приложения, выявив потенциальные уязвимости, и предложите меры по устранению.
9. Разработайте политику безопасности для мобильных устройств, используемых в организации.
10. Создайте сценарии кибератак, направленных на информационные ресурсы организации, и опишите меры по защите.
11. Разработайте модель управления доступом, обеспечивающую баланс между безопасностью и удобством использования.
12. Оцените безопасность корпоративных сетей в контексте подключенных устройств IoT и предложите меры по защите.
13. Проанализируйте уровень безопасности облачных сервисов, используемых организацией, и предложите рекомендации.
14. Предложите методы усиления идентификации и аутентификации пользователей в информационной системе.
15. Разработайте программу по формированию культуры безопасности среди сотрудников организации, включая обучение и мотивацию.

Итоговое тестирование (зачет):

1. Алгоритмы симметричного шифрования являются:
а) шифрованием с закрытым ключом
б) шифрованием с открытым ключом
в) шифрованием с двумя симметричными ключами

2. Что такое электронная подпись?
а) открытый ключ владельца

а) шифр замены
б) шифр перестановки
в) блочный шифр
г) потоковый шифр

5. В какому виду шифров относится один из древних шифров – шифр Цезаря?
а) шифр замены
б) шифр перестановки
в) блочный шифр
г) потоковый шифр

6. Что относится к критически важным принципам шифрования методом "одноразового шифроблокнота"?
а) ключ должен быть случайной последовательностью
б) длина ключа должна совпадать по размеру с длиной открытого текста
в) ключ может применяться только один раз
г) шифрование должно осуществляться открытым ключом, а расшифрование – закрытым.

7. Какая наука посвящена проблемам раскрытия шифров?
а) криптография
б) криптология
в) криптоанализ

8. Синоним симметричного шифрования:
а) шифрование с закрытым ключом
б) шифрование с открытым ключом
в) шифрование с двумя симметричными ключами

9. Чем по сути является электронная подпись?
а) открытым ключом владельца
б) закрытым ключом владельца
в) симметричным ключом
г) сертификатом проверки электронной подписи

10. Какое утверждение не верно для хэш-функции:
а) хеш-функция является детерминированной, то есть одно и то же сообщение приводит к одному и тому же хеш-значению
б) в отдельных случаях возможно найти два разных файла с одинаковым хеш-значением
в) незначительная корректировака файла может изменить хеш до неузнаваемости
г) значение хеш-функции быстро вычисляется для любого файла

11. Что такое информационная безопасность (выберете наиболее верное определение)
а) это защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры.
б) это практика предотвращения несанкционированного доступа информации.
в) это комплекс мер, которые нужны, чтобы защитить от утечки или взлома программы, компьютерные системы и данные.
г) это различные меры по защите информации от посторонних лиц.

12. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена
а) конфиденциальность
б) целостность
в) доступность
г) аутентичность
д) апеллируемость

13. Что из перечисленного является информацией с ограниченным доступом?
а) государственная тайна
б) персональные данные
в) достоверная информация
г) общедоступная информация

14. Установите соответствия терминов в области персональных данных с их определениями
I. сведения о расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни
II. сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность
III. фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, сообщаемые субъектом персональных данных с письменным согласием
IV. данные, хранимые в информационных системах в электронном виде, принадлежность которых конкретному субъекту персональных данных невозможно определить без дополнительной информации

а) сведения в военной области
б) сведения внешнеполитической области
в) сведения об экологии
г) сведения о военных потерях в мирное время

16. Какие грифы секретности могут быть у государственной тайны:
а) секретно, совершенно секретно, особой важности
б) секретно, совершенно секретно, доступ запрещен
в) строго конфиденциально, секретно, особой важности

17. Какие грифы секретности могут быть у коммерческой тайны:
а) секретно, совершенно секретно, особой важности
б) секретно, совершенно секретно, доступ запрещен
в) конфиденциально, секретно, совершенно секретно
г) у коммерческой тайны нет градации по разным грифам секретности

18. В чьи полномочия входит отнесение тех или иных сведений к государственной тайны?
а) министерства, ведомства, организации в пределах своих компетенций
б) только Правительства РФ и Президента РФ
в) только Государственной думы РФ и Совета Федерации РФ
г) только Президент РФ

19. Коммерческой тайной можно признать любую информацию, которая соответствует следующим условиям:
а) информация относится к предпринимательской деятельности компании и имеет для нее ценность
б) информацией не владеют третьи лица, но при этом она представляет реальную ценность для них
в) информация не принадлежит данной организации
г) обладатель такой информации ограничил доступ к ней и принял меры, чтобы защитить ее от несанкционированного доступа и распространения
д) информация содержит сведений, которые составляют государственную тайну

20. Выберете наиболее полное определение персональным данным (соответствующее законодательству):
а) любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу
б) информация, касающаяся личной жизни гражданина
в) сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность

Вопросы к экзамену:

Вопросы для проверки уровня обученности «знать»
1. Назовите три составляющие информационной безопасности.
2. Дайте определение обезличиванию персональных данных.
3. Перечислите виды алгоритмов шифрования.
4. Назовите, каким термином обозначается процедура проверки подлинности.
5. Свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации – это…
6. Перечислите виды электронной подписи.
7. Перечислите виды персональных данных в соответствии с Федеральным законом РФ № 152-ФЗ «О персональных данных»
8. Дайте определение персональным данным в соответствии с Федеральным законом РФ №152-ФЗ «О персональных данных».
9. Назовите, как называется государственный орган, муниципальный орган, юридическое или физическое лицо, осуществляющее обработку персональных данных.
10. Что необходимо выполнять для формирования архива данных, защищенного от изменений и повреждений, а также восстановления в случае повреждения или сбоев в первоисточнике?
11. Назовите криптографический алгоритм, который отображает данные произвольного размера в битовый массив фиксированного размера.
12. Перечислите, какие грифы секретности могут быть у государственной тайны.
13. Назовите вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей.
14. Назовите распределенную атаку, которая создаёт нагрузку на сервер и приводит к отказу системы.
15. Назовите метод шифрования данных, предполагающий использование двух ключей —открытого и закрытого.

Вопросы для проверки уровня обученности «уметь»
1. Охарактеризуйте определения доступности.
2. Сформулируйте определение конфиденциальности.
3. Сформулируйте определение целостности.
4. Дайте характеристику симметричному шифрованию (основной принцип)
5. Дайте характеристику асимметричному шифрованию (основной принцип)
6. Сформулируйте базовые правила безопасности при совершении финансовых операциях в онлайн-банках.

14. Сформулируйте определение термина «пен-тест».
15. Сформулируйте отличие «белого» хакеры от «черного».

Вопросы для проверки уровня обученности «владеть»
1. Зашифруйте текстовое сообщение с использованием симметричного алгоритма шифрования. Объясните выбор алгоритма и длины ключа.
2. Произведите процесс асимметричного шифрования для передачи конфиденциальной информации. Объясните преимущества использования асимметричных ключей.
3. Внедрите скрытое сообщение в изображение с использованием стеганографической техники. Расскажите о методе выбора места внедрения.
4. Создайте схему защиты от социальной инженерии, включая проведение тренингов и создание барьеров для атак данного вида.
5. Настройте брандмауэр для сетевого оборудования, обеспечивая защиту от внешних атак и нежелательного трафика.
6. Определите основные угрозы информационной безопасности в сценарии использования предприятия и предложите соответствующие контрмеры
7. Разработайте план резервного копирования, включая определение данных, регулярность копирования и место хранения.
8. Разработайте программу обучения сотрудников по основам информационной безопасности и проведите обучение с последующей оценкой знаний.
9. Проведите конфигурацию антивирусного ПО, включая определение расписания сканирования и настройку обновлений в режиме реального времени.
10. Разработайте стратегию защиты от фишинга и вредоносных вложений в электронной почте, включая использование антивирусных и антифишинговых фильтров.
11. Сравните различные средства шифрования электронной почты и предложите наилучший вариант для организации.
12. Предложите план интеграции различных систем мониторинга безопасности (логи, угрозы, события) для обеспечения централизованного управления.
13. Разработайте схему и политику регулярных обновлений программного обеспечения и операционных систем с учетом требований безопасности.
14. Определите и реализуйте эффективные методы аутентификации для мобильных устройств.
15. Создайте инцидентный план безопасности, включая шаги по обнаружению, реагированию и восстановлению после инцидента.

Итоговое тестирование (экзамен):

21. Как называется вид интернет-мошенничества, целью которого является получение идентификационных данных пользователей?
а) фишинг
б) вредоносное программное обеспечение
в) вишинг
г) смишинг

22. Что такое фарминг?
а) вид мошенничества, при котором вредоносный код устанавливается на ПК или сервер жертвы. Этот код меняет информацию по IP адресам, в результате чего обманутый пользователь перенаправляется на поддельные веб сайты без их ведома и согласия.
б) это такой метод, когда мошенники присылают SMS, как правило, о какой-нибудь выдуманной проблеме: застрявшей посылке, неоплаченном счете или заблокированном аккаунте. Чтобы решить проблему, нужно перейти по ссылке.
в) это метод атак несанкционированного доступа к информации или системам хранения информации без использования технических средств.

23. Что не относят к методам социальной инженерии?
а) DDos атаки
б) тайпсвотинг
в) претекстинг
г) "Квид про Кво"

24. В чем заключается основной принцип тайпсквоттинга?
а) эксплуатация опечатки при вводе веб-адреса в браузере
б) покупка веб адресов, написание которых аналогично названию других сайтов и брендов
в) рассылка писем, в которых есть некое "интересное" вложение
г) внедрение в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи

25. Какая самая распространенная угроза безопасности может быть при использовании электронной почты:
а) фишинговые рассылки
б) отслеживающие трекеры
в) угрозы отсутствуют
г) программы вирусы

а) внутренние
б) внешние
в) осведомленные
г) сетевые

30. . Соотнесите характеристику хакера с его цветом:
I. Специалисты по информационной безопасности (в частности специалистов, работающих в крупных IT компаниях) или исследователей IT систем, не нарушающих закон. Используют свои знания и навыки в вполне легальных и законных целях. Более того, их часто нанимают различные организации для проведения тестирования на проникновение и оценку уязвимости
II. Хакеры, которые являются еще пока новичками в хакерском мире, но при этом серьезно настроен повысить свои навыки в проведении кибер атак. В первую очередь сосредоточены на получении знаний о том, как проводить кибер атаки на том же уровне, что и их коллеги более высокого уровня
III. Нанимаются правительственными учреждениями для выявления уязвимостей в системах безопасности, уделяя особое внимание поиску и обезвреживанию хакеров
IV. Киберпреступники. Это настоящие профи в проникновении и нарушении компьютерной безопасности. Используют свои навыки для финансовой выгоды, ищут различные уязвимые места в системах крупных компаний для кражи данных, изменение данных или за уничтожение системы
V. Совершают мелкие нарушения законодательства или отсутствия нарушений законодательства, но нарушения внутренних правил какого-либо интернет сервиса
VI. Нанимаются организациями для проверки своих программ или сетей на наличие ошибок до их выпуска или внедрения. Роль таких хакеров заключается в том, чтобы находить лазейки или уязвимости в системе безопасности в новом программном обеспечении и устранять их до его запуска а. красные хакеры
б. серые хакеры
в. белые хакеры
г. зеленые хакеры
д. синие хакеры
е. черные хакеры

31. В чем заключается необратимое обезличивание персональных данных?
а) оператор уничтожает идентифицирующие данные, что не позволяет сделать даже ему процесс обезличивания обратимым, и использует эти данные для статистических, аналитических целей, таких, например, как андеррайтинг или исследование рынка
б) оператор заменяет информацию, идентифицирующую субъекта, например, ФИО и СНИЛС, некими условными идентификаторами, с сохранением возможности при необходимости связать обезличенные данные с конкретным субъектом

32. От чего зависит уровень защищенности ИСПДн?
а) от типа данных, от отношения с субъектами ПДн (сотрудники или не сотрудники), от количества субъектов ПДн, от типа актуальных угроз.
б) от типа данных, от территориального размещения, от наличия соединения с сетями общего пользования, от встроенных (легальных) операций с записями баз персональных данных, от объема ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки
в) от типа данных, от территориального размещения, от количества субъектов ПДн, от типа актуальных угроз.

33. Первый тип акуальных угроз означает, что это:
а) угрозы, связанные с недокументированными возможностями в прикладном ПО, например, в установленных программах
б) самые серьезные угрозы, связанные с недокументированными возможностями в системном программном обеспечении (ПО), например, в операционной системе
в) угрозы, не связанные с ПО, например, уязвимости в оборудовании

34. Какой орган проверяет соответствие требованиям для компании, обрабатывающей персональные данные?
а) Центробанк
б) Роскомнадзор
в) ФСБ
г) МВД

35. Аттестат соответствия 152 ФЗ позволяет хранить в облаке данные, которые требуют:
а) 1 уровня защищенности
б) 2 уровня защищенности
в) 3 уровня защищенности
г) 4 уровня защищенности

36. Вид злоумышленников, имеющих право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование информационной системы.
а) осведомленные
б) сетевые
в) внешние
г) внутренние

37. Кто такой информационный брокер?

а) собственную или контролируемую программную платформу (сетевую и ПК)
б) собственную аппаратную платформу (сетевую, мобильную и ПК)
в) собственную или контролируемую мобильную платформу
г) собственную медийную структуру СМИ, ТВ и Интернета

6.5. Примерная тематика курсовых работ (проектов)
Учебным планом не предусмотрено

6.6. Методические указания для обучающихся по освоению дисциплины (модуля)
Методические рекомендации по работе с конспектом лекций

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. 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 по структуре, оформлению и содержанию отчета по лабораторным и практическим работам.
Структура отчёта:
- цель работы;
- краткие теоретические сведения;
- ход выполнения работы;
- выводы.
Дополнительными 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, дипломная работа):
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 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.

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 учебной дисциплине (разделу). 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 учебной дисциплине. 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. В самом начале учебного курса познакомьтесь со следующей учебно-методической документацией:
- программой дисциплины;
- 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. Систематическое выполнение учебной работы на лекциях и лабораторных занятиях позволит успешно освоить дисциплину 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	Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]:учебник для вузов. - Санкт-Петербург: Лань, 2023. - 124 с. – Режим доступа: https://e.lanbook.com/book/293009
Л.1.2	Никифоров С. Н. Методы защиты информации. Шифрование данных [Электронный ресурс]:учебное пособие. - Санкт-Петербург: Лань, 2019. - 160 с. – Режим доступа: https://e.lanbook.com/book/114699
7.2. Лицензионное и свободно распространяемое программное обеспечение в том числе отечественного производства	
7.2.1	Microsoft Windows 10
7.2.2	Microsoft Office 2013 Standard
7.2.3	Kaspersky Endpoint Security
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	"Электронная библиотека учебников" . Режим доступа: http://studentam.net/
7.3.5	Компьютерная справочно-правовая система "КонсультантПлюс". Режим доступа: http://www.consultant.ru/

7.3.6	ПЛАТФОРМА ОНЛАЙН-ОБРАЗОВАНИЯ «РАЗУМ». Режим доступа: https://razoom.mgutm.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

9. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ

Организация образовательного процесса для лиц с ограниченными возможностями 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
канд. экон. наук, доц. Мурат Е.П._____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры

Физика, математика и информационные технологии

Протокол от __ _____ 2025 г. № __
Зав. кафедрой Нечушкин Александр Юрьевич_____

Рабочая программа согласована на заседании выпускающей кафедры

Физика, математика и информационные технологии

Протокол от __ _____ 2025 г. № __
Зав. кафедрой Нечушкин Александр Юрьевич _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
канд. экон. наук, доц. Мурат Е.П._____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры

Физика, математика и информационные технологии

Протокол от __ _____ 2026 г. № __
Зав. кафедрой Нечушкин Александр Юрьевич_____

Рабочая программа согласована на заседании выпускающей кафедры

Физика, математика и информационные технологии

Протокол от __ _____ 2026 г. № __
Зав. кафедрой Нечушкин Александр Юрьевич _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
канд. экон. наук, доц. Мурат Е.П._____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры

Физика, математика и информационные технологии

Протокол от __ _____ 2027 г. № __
Зав. кафедрой Нечушкин Александр Юрьевич_____

Рабочая программа согласована на заседании выпускающей кафедры

Физика, математика и информационные технологии

Протокол от __ _____ 2027 г. № __
Зав. кафедрой Нечушкин Александр Юрьевич _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
канд. экон. наук, доц. Мурат Е.П._____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры

Физика, математика и информационные технологии

Протокол от __ _____ 2028 г. № __
Зав. кафедрой Нечушкин Александр Юрьевич_____

Рабочая программа согласована на заседании выпускающей кафедры

Физика, математика и информационные технологии

Протокол от __ _____ 2028 г. № __
Зав. кафедрой Нечушкин Александр Юрьевич _____