МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Смоленский казачий институт промышленных технологий и бизнеса (филиал) федерального государственного бюджетного образовательного учреждения «Московский государственный университет технологий и управления имени К.Г. Разумовского (Первый казачий университет)»

УТВЕРЖДАЮ
Директор СКИПТБ (филиал) ФГБОУ ВО
«МГУТУ им. К.Г. Разумовского (ПКУ)
_____ Н.С. Коржикова
«21» апреля 2025 г.

Рабочая программа дисциплины (модуля)

Б1.О.04.10 ОБЩЕПРОФЕССИОНАЛЬНЫЙ МОДУЛЬ Информационная безопасность

Кафедра:	Системной автоматизации и информационных технологий
Направление подготовки:	09.03.01 Информатика и вычислительная техника
Направленность (профиль):	Проектирование программного обеспечения
Квалификация выпускника:	Бакалавр
Форма обучения:	заочная
Год набора:	2025
Общая трудоемкость:	216 часов/6 з.е.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00b895e5d3e87e5e81c0f723de8ac92877
Действителен: с 06.08.2024 по 30.10.2025
Владелец: **Коржикова Надежда Сергеевна**
Должность: **Директор**

Вязьма, 2025 г.

Программу составил(и):
к.п.н. доцент Анурьева Мария Сергеевна
к.п.н доцент Кузьмин Константин Анатольевич

Рабочая программа дисциплины (модуля)
"Информационная безопасность"
разработана на основании учебного плана, утвержденного ученым советом 27 марта 2025 г. протокол № 9 в соответствии
с ФГОС ВО Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. № 929)

Руководитель ОПОП
канд. пед. наук, доцент Кузьмин К.А._____

Рабочая программа обсуждена на заседании обеспечивающей кафедры
Системной автоматизации и информационных технологий
Протокол от 14 апреля 2025 г. № 9
Зав. кафедрой Кузьмин Константин Анатольевич_____

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 КУРСАМ

Цикл (раздел) ОП: Б1.О

Дисциплина относится к обязательной части ОПОП и обязательна для освоения.

Распределение часов дисциплины

Курс	4		Итого	
Вид занятий	УП	РП		
Лекции	4	4	4	4
Лабораторные	8	8	8	8
Практические	4	4	4	4
В том числе в форме практ.подготовки	2	2	2	2
Итого ауд.	16	16	16	16
Контактная работа	16	16	16	16
Сам. работа	187	187	187	187
Часы на контроль	13	13	13	13
Итого	216	216	216	216

Вид промежуточной аттестации:

Экзамен 4 курс

Зачёт 4 курс

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С РЕЗУЛЬТАТАМИ ОСВОЕНИЯ 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 информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности 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 методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименования разделов, тем, их краткое содержание и результаты освоения /вид занятия/	Курс	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 ЗНАТЬ основы криптографической защиты информации (симметричное и ассиметричное шифрование, хэш-функции, электронная подпись) /Лек/**	4	2	0	0	ОПК-3.1	устный опрос
1.2	**Лабораторная работа 1.1. Сравнение данных с помощью хэш-функции Краткое содержание: Изучение принципов работы хэш-функций и их применение для сравнения данных. Освоение методов вычисления хэш-сумм файлов и текстовых данных. Практическое применение алгоритмов MD5, SHA-1, SHA-256, SHA-512 для проверки целостности данных и выявления совпадений. Предполагаемые результаты обучения: УМЕТЬ: - Вычислять хэш-суммы различных типов данных - Сравнивать файлы на предмет идентичности по их хэш-суммам - Применять различные алгоритмы хэширования - Определять целостность данных с помощью хэш-функций**	4	2	0	0	ОПК-3.2,ОПК-3.3	задания к лабораторной работе

	ВЛАДЕТЬ: **- Навыками работы с программными средствами для вычисления хэш-сумм** **- Методами проверки целостности данных** **- Техникой сравнения файлов на основе их хэш-значений** **- Практическими навыками использования современных хэш-алгоритмов** **/Лаб/**						
1.3	**Лабораторная работа 1.2 . Стеганографические методы защиты информации** **Краткое содержание:** **Изучение методов скрытой передачи информации. Освоение практических навыков внедрения данных в графические, аудио- и видеофайлы. Применение программных средств для стеганографии. Анализ защищенности стеганографических сообщений.** **Предполагаемые результаты обучения:** **УМЕТЬ:** **- Внедрять информацию в различные типы медиафайлов** **- Извлекать скрытые данные из носителей** **- Оценивать степень защищенности стеганографических сообщений** **- Выбирать оптимальные методы стеганографии для конкретных задач** **ВЛАДЕТЬ:** **- Навыками работы со стеганографическими программами** **- Методами анализа защищенности скрытых данных** **- Техникой внедрения и извлечения информации** **- Практическими навыками оценки эффективности стеганографических методов** **/Лаб/**	4	2	0	0	ОПК-3.2,ОПК-3.3	задания к лабораторной 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 повышения безопасности информационных систем.** **Предполагаемые результаты обучения:**	4	62	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы для самоподготовки

	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	**Практическая работа 2.1. Организация защиты персональных данных Краткое содержание: Изучение нормативно-правовой базы в области защиты персональных данных. Освоение методов классификации и категорирования информации. Практическое применение технических средств защиты ПД. Настройка политик безопасности для работы с персональными данными. Предполагаемые результаты обучения: УМЕТЬ: – Классифицировать персональные данные по категориям – Определять требования к защите различных категорий ПД – Настраивать средства защиты информации – Разрабатывать политики безопасности для работы с ПД – Применять технические меры защиты персональных данных ВЛАДЕТЬ: – Навыками работы с нормативными документами в области защиты ПД – Методами оценки рисков при работе с персональными данными – Техникой настройки средств защиты информации – Практическими навыками разработки регламентов по защите ПД – Методами контроля соблюдения**	4	2	0	2	ОПК-3.2,ОПК-3.3	тестирование

	требований по защите персональных данных /Пр/						
2.2	**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: – Классифицировать персональные данные по категориям – Определять требования к защите различных категорий ПД – Настраивать средства защиты информации – Разрабатывать политики безопасности для работы с ПД – Применять технические меры защиты персональных данных ВЛАДЕТЬ: – Навыками работы с нормативными документами в области защиты ПД – Методами оценки рисков при работе с персональными данными – Техникой настройки средств защиты информации – Практическими навыками разработки регламентов по защите ПД – Методами контроля соблюдения требований по защите персональных данных /Ср/**	4	62	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	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-**	4	2	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	**Практическая работа 3.1. Блокирование рекламы и нежелательных объектов на веб-страницах Краткое содержание: Блокирование рекламы и нежелательных объектов на веб-страницах с помощью утилиты Adguard, AdblockPlus. 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 /Пр/**	4	2	0	0	ОПК-3.2,ОПК-3.3	тестирование
3.3	**Лабораторная работа 3.2. Исследование методов защиты паролей пользователя Краткое содержание Изучение основных методов защиты паролей пользователя и формирование навыков создания надежных паролей Предполагаемые результаты обучения: УМЕТЬ анализировать существующие пароли по заданным критериям, создавать надежные пароли, соблюдая следующие правила ВЛАДЕТЬ: Навыками работы с менеджерами паролей, методами оценки стойкости паролей /Лаб/**	4	2	0	0	ОПК-3.2,ОПК-3.3	задания к лабораторной работе
3.4	**Лабораторная работа 3.3. Антивирусное программное обеспечение Краткое содержание: Изучение принципов работы антивирусных программ. Освоение методов обнаружения и удаления вредоносного ПО. Практическое применение различных типов антивирусной защиты. Настройка параметров сканирования и мониторинга системы. Предполагаемые результаты обучения: УМЕТЬ: – Настраивать параметры антивирусной защиты – Проводить полное и выборочное сканирование системы**	4	2	0	0	ОПК-3.2,ОПК-3.3	задания к лабораторной работе

	– Анализировать результаты антивирусной проверки – Устранять обнаруженные угрозы – Обновлять базы сигнатур и антивирусные компоненты – Оценивать эффективность антивирусной защиты ВЛАДЕТЬ: – работы с различными типами антивирусного ПО – Методами обнаружения и нейтрализации вредоносных программ – Техникой настройки профилей безопасности – Практическими навыками мониторинга защищенности системы – Методами анализа логов антивирусной защиты – Способностью оценивать риски заражения системы вредоносным ПО /Лаб/						
3.5	**Информационная безопасность пользователя Самостоятельная работа по теме "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 использовать современные информационно-коммуникационные средства блокирования рекламы и нежелательных объектов на веб-страницах, анализировать существующие пароли по заданным критериям, создавать надежные пароли, соблюдая следующие правила – Настраивать параметры антивирусной защиты – Проводить полное и выборочное сканирование системы – Анализировать результаты антивирусной проверки – Устранять обнаруженные угрозы – Обновлять базы сигнатур и антивирусные компоненты – Оценивать эффективность антивирусной защиты ВЛАДЕТЬ: навыками выбора наилучших методов блокирования рекламы и нежелательных**	4	63	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы для самоподготовки

	объектов на веб-страницах, Навыками работы с менеджерами паролей, методами оценки стойкости паролей – навыками работы с различными типами антивирусного ПО – Методами обнаружения и нейтрализации вредоносных программ – Техникой настройки профилей безопасности – Практическими навыками мониторинга защищенности системы – Методами анализа логов антивирусной защиты – Способностью оценивать риски заражения системы вредоносным ПО /Ср/						
	Раздел 4.Промежуточный контроль						
4.1	**Зачёт с оценкой ОПК-2.1: Знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); современные инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, используемые для решения задач профессиональной деятельности, и принципы их работы ОПК-2.2: Умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства, в том числе отечественного производства, для решения задач профессиональной деятельности; анализировать профессиональные задачи, выбирать и использовать подходящие информационные технологии ОПК-2.3: Владеет навыками работы с данными с помощью информационных технологий; навыками применения современных информационно-коммуникационных и интеллектуальных технологий, инструментальных сред, программно-технических платформ и программных средств, в том числе отечественного производства, для решения задач профессиональной деятельности /Зачёт/**	4	4	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы к зачету, итоговое тестирование
4.2	**Экзамен ОПК-3: Способен решать стандартные задачи профессиональной деятельности на**	4	9	0	0	ОПК-3.1,ОПК-3.2,ОПК-3.3	вопросы к экзамену, итоговое тестирование

	основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; ОПК-3.1: Знает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности 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 методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и требований информационной безопасности /Экзамен/						

Перечень применяемых активных и интерактивных образовательных технологий:

Информационные технологии

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

Проектная технология

Стандартизированный метод оценки знаний, умений, навыков учащихся, который помогает выявить и сформировать индивидуальный темп обучения, пробелы в текущей итоговой подготовке

Технология модульного обучения

Технология модульного обучения основана на идее личностно-ориентированного подхода. Основной технологии модульного обучения является самостоятельное освоение учебных дисциплин, которые для удобства поделены на модули. Цель технологии модульного обучения – создать условия выбора для полного овладения содержанием образовательных программ в разной последовательности, разном объеме и темпе через отдельные и независимые учебные модули с учетом индивидуальных интересов и возможностей субъектов образовательного процесса

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:

Знает принципы информационной культуры

Умеет решать стандартные задачи профессиональной деятельности

Владеет методами поиска и анализа информации для подготовки документов

Пороговый уровень:

Знает принципы информационной и библиографической культуры

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

Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций

Продвинутый уровень:

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

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

Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры

Высокий уровень:

Знает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности 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 методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и 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
Знает принципы информационной культуры
Умеет решать стандартные задачи профессиональной деятельности
Владеет методами поиска и анализа информации для подготовки документов
2. Пороговый уровень
Знает принципы информационной и библиографической культуры
Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры
Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций
3. Продвинутый уровень
Знает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности
Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий
Владеет методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры
4. Высокий уровень
Знает принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности 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 методами поиска и анализа информации для подготовки документов, обзоров, рефератов, докладов, публикаций, на основе информационной и библиографической культуры с учетом соблюдения авторского права и 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 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 принципы лежат в основе классических криптографических методов?
Каковы основные особенности шифра Цезаря и как он работает?
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?

Задания к лабораторным и практическим работам
Лабораторная работа 1.1. Сравнение данных с помощью хэш-функции
1. Вычислить хэш-суммы файла с помощью алгоритмов MD5, SHA-1 и SHA-256.
2. Создать копию файла и внести в него однобайтовое изменение.
3. Сравнить исходные и измененные хэш-суммы, проанализировать результаты.
4. Сгенерировать хэш-суммы для текстового файла и его зашифрованной версии.
5. Сравнить полученные результаты, сделать выводы о стойкости алгоритмов.
Лабораторная работа 1.2. Стеганографические методы защиты информации
1. Внедрить текстовый файл в графический формат BMP.
2. Спрятать аудиофайл в видеоформате MP4.
3. Извлечь внедренные данные и проверить их целостность.
4. Оценить степень защищенности стеганографических сообщений.
5. Провести анализ влияния стеганографии на качество носителя.
Практическая работа 2.1. Организация защиты персональных данных
1. Классифицировать имеющийся массив персональных данных.
2. Настроить разграничение доступа к различным категориям ПД.
3. Реализовать шифрование конфиденциальных данных.
4. Настроить аудит действий с персональными данными.
5. Составить политику безопасности для работы с ПД.
Практическая работа 3.1. Блокирование рекламы
1. Установить и настроить Adguard для браузера.
2. Настроить AdblockPlus для блокировки рекламы.
3. Создать собственный список фильтров.
4. Проверить эффективность блокировки на различных сайтах.
5. Оценить влияние блокировщиков на производительность.
Лабораторная работа 3.2. Исследование методов защиты паролей
1. Создать набор паролей разной сложности.
2. Проверить их на устойчивость к брутфорс-атакам.
3. Оценить эффективность методов хранения паролей.
4. Исследовать работу менеджера паролей.
5. Сформировать рекомендации по созданию надежных паролей.
Лабораторная работа 3.3. Антивирусное программное обеспечение
1. Настроить антивирусную защиту системы.
2. Провести полное сканирование системы.
3. Обработать обнаруженные угрозы.
4. Настроить режим реального времени.
5. Оценить влияние антивируса на производительность системы.

Тестирование

Практическая работа 2.1. Организация защиты персональных данных
1. Какие категории персональных данных существуют согласно законодательству?
а) Общедоступные
б) Биометрические
в) Специальные
г) Все вышеперечисленные
2. Кто является оператором персональных данных?
а) Физическое лицо
б) Юридическое лицо
в) Государственный орган

г) Все вышеперечисленные
3. Какие способы классификации ПД существуют?
а) По степени конфиденциальности
б) По объему обрабатываемых данных
в) По способу хранения
г) Все вышеперечисленные
4. Какие технические средства защиты ПД являются обязательными?
а) Антивирусное ПО
б) Межсетевой экран
в) Система резервного копирования
г) Все вышеперечисленные
5. Что такое политика безопасности ПД?
а) Документ с правилами обработки
б) Программное обеспечение
в) Организационная структура
г) Метод шифрования
6. Какие действия требуют согласия субъекта ПД?
а) Сбор данных
б) Обработка данных
в) Распространение данных
г) Все вышеперечисленные
7. Какие меры защиты применяются к специальным категориям ПД?
а) Усиленное шифрование
б) Ограниченный доступ
в) Регулярный аудит
г) Все вышеперечисленные
8. Что такое конфиденциальность ПД?
а) Доступность данных
б) Целостность данных
в) Защита от несанкционированного доступа
г) Все вышеперечисленное
9. Какие действия запрещены при обработке ПД?
а) Сбор без согласия
б) Распространение без разрешения
в) Хранение без необходимости
г) Все вышеперечисленные
10. Какие права имеет субъект ПД?
а) На доступ к своим данным
б) На исправление данных
в) На удаление данных
г) Все вышеперечисленные
11. Какие виды аудита применяются к обработке ПД?
а) Внутренний
б) Внешний
в) Государственный
г) Все вышеперечисленные
12. Что такое шифрование ПД?
а) Преобразование данных в непонятный вид
б) Метод хранения данных
в) Способ передачи данных
г) Система доступа к данным
13. Какие технические средства защиты обязательны при передаче ПД?
а) VPN-соединение
б) SSL-шифрование
в) Двухфакторная аутентификация
г) Все вышеперечисленные
14. Что такое локализация ПД?
а) Хранение данных в определенной стране
б) Ограничение доступа к данным
в) Шифрование данных
г) Резервное копирование
15. Какие действия необходимо предпринять при утечке ПД?
а) Информирование регуляторов
б) Уведомление субъектов ПД
в) Устранение причин утечки
г) Все вышеперечисленные
Дополнительные вопросы для углубленного понимания:
16. Какие сроки хранения ПД установлены законодательством?
а) Не более 3 лет

б) Не более 5 лет
в) В течение срока действия договора
г) По усмотрению оператора
17. Какие санкции предусмотрены за нарушение ФЗ о ПД?
а) Предупреждение
б) Штрафы
в) Приостановление деятельности
г) Все вышеперечисленные
18. Что такое анонимизация ПД?
а) Удаление персональных данных
б) Замена персональных данных
в) Шифрование персональных данных
г) Все вышеперечисленные
19. Какие требования предъявляются к сотрудникам, работающим с ПД?
а) Прохождение инструктажа
б) Подписание соглашения о конфиденциальности
в) Наличие допуска
г) Все вышеперечисленные
20. Какие способы передачи ПД разрешены законом?
а) По защищенному каналу связи
б) Через курьерскую доставку
в) По почте с уведомлением
г) Все вышеперечисленные при соблюдении требований безопасности

Практическая работа 3.1. Блокирование рекламы и нежелательных объектов на веб-страницах
1. Какие браузерные расширения используются для блокировки рекламы?
а) Adblock Plus
б) uBlock Origin
в) Ghostery
г) Adguard
2. Что такое фильтр рекламы?
а) Список правил для блокировки контента
б) Программа для очистки браузера
в) Метод шифрования данных
г) Инструмент для ускорения загрузки
3. Какие типы рекламы блокируются стандартными фильтрами?
а) Поп-ап окна
б) Видеореклама
в) Баннеры
г) Контекстная реклама
4. Как можно создать собственный фильтр?
а) Изменить существующий
б) Написать с нуля
в) Использовать готовые шаблоны
г) Скопировать чужой
5. Какие методы обхода блокировщиков используют рекламодатели?
а) Маскировка под контент
б) Динамическая загрузка
в) Использование JavaScript
г) Изменение доменных имен
6. Что такое белый список?
а) Список разрешенных сайтов
б) Список заблокированных сайтов
в) Список фильтров
г) Список безопасных расширений
7. Какие преимущества дает использование блокировщиков?
а) Ускорение загрузки страниц
б) Экономия трафика
в) Защита от вредоносного контента
г) Улучшение внешнего вида сайтов
8. Какие недостатки есть у блокировщиков рекламы?
а) Снижение производительности
б) Конфликт с сайтами
в) Блокировка полезного контента
г) Потребление дополнительного трафика
9. Как проверить эффективность блокировки?
а) Открыть страницу без блокировщика
б) Использовать инструменты разработчика
в) Проверить список заблокированных элементов

г) Просмотреть статистику блокировщика
10. Какие типы контента можно блокировать дополнительно?
а) Социальные кнопки
б) Аналитические трекеры
в) Комментарии
г) Рекламные баннеры
11. Что такое префильтр?
а) Предварительный фильтр для блокировки
б) Инструмент для создания фильтров
в) Метод шифрования данных
г) Система уведомлений
12. Какие форматы рекламы блокируются автоматически?
а) HTML-баннеры
б) Flash-реклама
в) Видеореклама
г) Текстовая реклама
13. Как обновить фильтры?
а) Вручную
б) Автоматически
в) Через настройки расширения
г) С помощью сторонних программ
14. Какие инструменты используются для анализа заблокированного контента?
а) Статистика блокировщика
б) Консоль браузера
в) Отчеты о блокировках
г) Системный журнал
15. Что такое пользовательский скрипт?
а) Пользовательский фильтр
б) Пользовательский стиль
в) Пользовательская функция
г) Пользовательский шаблон

6.4. Оценочные средства промежуточной аттестации.

Вопросы к зачёту
Индикатор Знать
1) Установите правильную последовательность развития методов шифрования:
а) Появление симметричных шифров
б) Изобретение шифра Цезаря
в) Создание шифрмашины Энигма
г) Разработка асимметричных шифров
2) Прочитайте текст и установите соответствие между терминами и их определениями:
А) Криптология
Б) Криптоанализ
В) Криптография
Г) Шифр
1. Наука о методах обеспечения конфиденциальности информации
2. Наука о методах вскрытия шифров
3. Общая наука о шифрах и методах их анализа
4. Система преобразования информации для обеспечения секретности
5. Метод аутентификации пользователей
3) Установите правильную последовательность появления шифров:
а) Шифр Виженера
б) Решетка Кардано
в) Шифр Цезаря
г) Одноразовый шифр-блокнот
4) Прочитайте текст и установите соответствие между методами и их характеристиками:
А) Симметричное шифрование
Б) Асимметричное шифрование
В) Цифровая подпись
Г) Атака “человек посередине”
1. Требует двух ключей для работы
2. Использует один ключ для шифрования и дешифрования
3. Обеспечивает аутентификацию и целостность
4. Представляет угрозу безопасности передачи данных
5. Метод стеганографии

5) Установите правильную последовательность этапов развития криптографии:
а) Появление механических шифрмашин
б) Развитие математических основ защиты
в) Изобретение электромагнитного телеграфа
г) Формирование научных методов защиты
6) Прочитайте текст и установите соответствие между терминами и их применением:
А) Сертификат
Б) УЦ (Удостоверяющий центр)
В) Ключ
Г) Протокол
1. Инструмент для шифрования данных
2. Документ, подтверждающий личность
3. Система правил для безопасной передачи данных
4. Организация, выдающая цифровые сертификаты
5. Метод криптоанализа
7) Установите правильную последовательность развития технологий:
а) Появление цифровых подписей
б) Развитие симметричных шифров
в) Создание шифрмашины Энигма
г) Внедрение асимметричных шифров
8) Прочитайте текст и установите соответствие между методами и их особенностями:
А) Шифр Цезаря
Б) Шифр Виженера
В) Решетка Кардано
Г) Одноразовый блокнот
1. Использует таблицу для шифрования
2. Основан на сдвиге букв
3. Применяет периодическую замену
4. Обеспечивает абсолютную секретность
5. Метод перестановки
9) Установите правильную последовательность появления технологий:
а) Появление сертификатов
б) Развитие УЦ
в) Внедрение цифровых подписей
г) Создание шифрмашин
10. Прочитайте текст и установите соответствие между терминами и их функциями:
А) Стенография
Б) Криптография
В) Цифровая подпись
Г) Сертификат
1. Метод криптоанализа
2. Метод шифрования данных
3. Инструмент аутентификации
4. Документ подтверждения личности
5. Метод скрытой передачи информации
Индикатор Уметь
11) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод шифрования обеспечивает абсолютную секретность?
а) Шифр Цезаря
б) Шифр Виженера
в) Одноразовый шифр-блокнот
г) Симметричное шифрование
12) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие методы шифрования используют два ключа?
а) Асимметричное шифрование
б) Симметричное шифрование
в) Шифр Энигма
г) Цифровая подпись
13) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое криптоанализ?
а) Наука о методах шифрования
б) Наука о методах вскрытия шифров
в) Метод стеганографии
г) Технология создания ключей
14) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие характеристики присущи симметричному шифрованию?
а) Использование одного ключа
б) Высокая скорость работы
в) Сложность в управлении ключами

г) Использование двух ключей
15) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод защиты информации относится к стеганографии?
а) Шифр Цезаря
б) Решетка Кардано
в) Метод скрытой передачи данных
г) Шифр Виженера
16) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие преимущества имеет асимметричное шифрование?
а) Высокая скорость шифрования
б) Простота в управлении ключами
в) Возможность безопасной передачи ключей
г) Использование одного ключа
17) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое атака “человек посередине”?
а) Метод шифрования данных
б) Метод криптоанализа
в) Метод перехвата и изменения данных
г) Метод аутентификации
18) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие функции выполняет цифровая подпись?
а) Подтверждение авторства
б) Обеспечение конфиденциальности
в) Проверка целостности данных
г) Шифрование сообщений
19) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое криптографический протокол?
а) Метод шифрования данных
б) Система правил для безопасной передачи данных
в) Технология создания ключей
г) Метод криптоанализа
20) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие характеристики присущи шифрмашине Энигма?
а) Механическое устройство
б) Использование симметричного шифрования
в) Применение асимметричного шифрования
г) Автоматическая генерация ключей

Индикатор Владеть
21) Прочитайте текст и запишите развернутый ответ: В ходе исторического исследования были обнаружены зашифрованные послания, использовавшие шифр сцитала. Объясните принцип работы этого шифра и предположите, почему он считался надежным в свое время. Какие недостатки были у этого метода шифрования?
22) Рассчитайте количество возможных вариантов ключа для шифра Цезаря, если известно, что в алфавите используется 33 символа. Объясните, почему данный шифр считается уязвимым для современных методов криптоанализа.
23) Определите, какой метод шифрования использовался в следующем сообщении: “БМЪЛЪЖЪПЪ” (исходное сообщение “АЛФАВИТ”). Опишите алгоритм расшифровки и объясните, почему этот метод считается более надежным, чем простой шифр Цезаря.
24) Вычислите длину ключевого слова для шифра Виженера, если известно, что в зашифрованном тексте длиной 100 символов обнаружено 20 повторений определенных буквенных комбинаций через равные промежутки.
25) Прочитайте текст и запишите развернутый обоснованный ответ: В 1940-х годах немецкая армия использовала шифровальную машину “Энигма”. Объясните принцип работы этой машины и почему она считалась практически неуязвимой. Какие факторы привели к ее взлому?
26) Определите, какой метод шифрования является более надежным: симметричный или асимметричный. Приведите примеры использования каждого метода в современном мире и объясните их преимущества и недостатки.
27) Рассчитайте количество возможных комбинаций ключей для симметричного алгоритма шифрования, если длина ключа составляет 128 бит. Объясните, почему такая длина считается достаточной для обеспечения безопасности данных.
28) Прочитайте текст и запишите развернутый ответ: В процессе передачи данных через незащищенный канал была обнаружена атака “человек посередине”. Опишите механизм этой атаки и предложите методы защиты от нее.
29) Определите, какие преимущества дает использование “одноразового шифрблокнота” по сравнению с другими методами шифрования. Объясните, почему этот метод считается абсолютно надежным, несмотря на свои недостатки.
30) Вычислите время, необходимое для взлома асимметричного ключа длиной 2048 бит при современных вычислительных мощностях. Объясните, почему асимметричное шифрование используется преимущественно для обмена симметричными ключами, а не для шифрования самих данных.

Вопросы к экзамену
Индикатор Знать
1) Установите правильную последовательность этапов работы с персональными данными:
а) Классификация информации
б) Настройка политик безопасности
в) Применение технических средств защиты

а) Фишинг
б) Претекстинг
в) Квид про Кво
г) Обратная социальная инженерия
4) Прочитайте текст и установите соответствие между типами вредоносного ПО и их характеристиками:
А) Троянский конь
Б) Шпионское ПО
В) Вирус
Г) Червь
1. Самовоспроизводящееся ПО
2. ПО, маскирующееся под полезное
3. ПО для сбора информации
4. Самораспространяющееся ПО
5. ПО для майнинга криптовалюты
5) Установите правильную последовательность действий при настройке безопасности:
а) Создание политик паролей
б) Внедрение антивирусной защиты
в) Настройка файрвола
г) Регулярное резервное копирование
6) Прочитайте текст и установите соответствие между методами защиты и их применением:
А) Двухфакторная аутентификация
Б) Шифрование данных
В) Антивирусная защита
Г) Фильтрация контента
1. Защита от вредоносного ПО
2. Защита при передаче данных
3. Усиленная аутентификация
4. Контроль доступа к информации
5. Защита от DDoS-атак
7) Установите правильную последовательность действий при обнаружении утечки данных:
а) Уведомление регуляторов
б) Оценка масштаба утечки
в) Устранение причин
г) Информирование субъектов ПД
8) Прочитайте текст и установите соответствие между типами паролей и их характеристиками:
А) Простой пароль
Б) Композитный пароль
В) Фраза-пароль
Г) Биометрический пароль
1. Использование нескольких типов символов
2. Использование отпечатка пальца
3. Использование простой комбинации
4. Использование длинной фразы
5. Использование графического ключа
9) Установите правильную последовательность методов сбора информации:
а) Анализ открытых источников
б) Социальная инженерия
в) Физический доступ
г) Кибербразведка
10) Прочитайте текст и установите соответствие между методами защиты и их функциями:
А) VPN
Б) SSL-шифрование
В) Брандмауэр
Г) Антивирус
1. Защита при передаче данных
2. Контроль сетевого трафика
3. Защита от вредоносного ПО
4. Защита веб-соединений
5. Защита от DoS-атак

Индикатор Уметь
11) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Какой метод защиты информации относится к техническим средствам?
а) Классификация данных
б) Антивирусная защита
в) Политика безопасности
г) Обучение персонала
12) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие характеристики относятся к стойкому паролю?

а) Использование только букв
б) Длина не менее 12 символов
в) Комбинация разных типов символов
г) Простой словарный пароль
13) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое фишинг?
а) Метод физического доступа к устройству
б) Метод социальной инженерии с подменными сайтами
в) Метод криптоанализа
г) Метод стеганографии
14) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие методы относятся к вредоносному ПО?
а) Троянский конь
б) Антивирус
в) Вирус
г) Файрвол
15) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое претекстинг?
а) Метод анализа клавиатурного почерка
б) Метод получения информации через создание ложной ситуации
в) Метод обмена информацией
г) Метод фишинга
16) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие способы защиты от вредоносного ПО существуют?
а) Использование антивируса
б) Регулярное резервное копирование
в) Двухфакторная аутентификация
г) Обновление ПО
17) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое обратная социальная инженерия?
а) Метод сбора информации из открытых источников
б) Метод, при котором жертва сама предоставляет информацию
в) Метод фишинга
г) Метод претекстинга
18) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие характеристики относятся к политике безопасности?
а) Правила доступа к информации
б) Методы шифрования данных
в) Порядок реагирования на инциденты
г) Технические средства защиты
19) Выберите правильный ответ из предложенных вариантов и обоснуйте свой выбор:
Что такое “дорожное яблоко”?
а) Метод фишинга
б) Метод социальной инженерии с использованием заражённых носителей
в) Метод претекстинга
г) Метод криптоанализа
20) Выберите правильные ответы и запишите аргументы, обосновывающие выбор ответа:
Какие методы относятся к классификации информации?
а) Определение уровней конфиденциальности
б) Настройка файрвола
в) Категорирование по степени важности
г) Использование VPN

Индикатор Владеть
21) Прочитайте текст и запишите развернутый ответ: В организации произошел инцидент с утечкой персональных данных. Определите, какие нормативные акты были нарушены и какие меры наказания могут последовать согласно действующему законодательству.
22) Рассчитайте минимальный срок хранения журналов регистрации событий информационной безопасности, если организация обрабатывает специальные категории персональных данных. Обоснуйте свой ответ со ссылкой на законодательство.
23) Определите категорию конфиденциальности информации, если в документе содержатся персональные данные 1000 сотрудников, включая банковские реквизиты. Объясните выбор категории с учетом возможных рисков утечки.
24) Вычислите количество возможных комбинаций для пароля, состоящего из 8 символов (буквы, цифры, спецсимволы). Оцените его стойкость к подбору и предложите рекомендации по усилению.
25) Прочитайте текст и запишите развернутый обоснованный ответ: В компанию поступил подозрительный email от “банковского сервиса”. Опишите признаки фишингового сообщения и предложите алгоритм действий сотрудника при получении подобных писем.
26) Определите, какой метод социальной инженерии использовался, если злоумышленник представился сотрудником техподдержки и запросил пароль от учетной записи. Объясните, почему этот метод эффективен и как от него защититься.
27) Рассчитайте время, необходимое для подбора пароля, состоящего из 12 случайных символов, при скорости 1 миллиард попыток в секунду. Оцените практическую стойкость такого пароля.
28) Прочитайте текст и запишите развернутый ответ: В организации обнаружены следы вредоносного ПО. Определите

б) Криптография использует открытые ключи, криптоанализ - закрытые
в) Криптография работает с текстом, криптоанализ - с числами
г) Криптография использует только симметричные методы
2. Какой шифр относится к методам перестановки?
а) Шифр Цезаря
б) Шифр Виженера
в) Шифр сциталя
г) Решетка Кардано
3. Что такое одноразовый шифр-блокнот?
а) Симметричный шифр
б) Асимметричный шифр
в) Абсолютно секретный шифр
г) Метод стеганографии
4. Какие преимущества имеет асимметричное шифрование?
а) Высокая скорость работы
б) Простота реализации
в) Возможность безопасной передачи ключей
г) Низкая ресурсоемкость
5. Что такое атака “человек посередине”?
а) Перехват и изменение передаваемых данных
б) Кража ключей шифрования
в) Взлом криптосистемы
г) Социальная инженерия
6. Какой метод шифрования использует таблицу Виженера?
а) Метод замены
б) Метод перестановки
в) Метод гаммирования
г) Метод стеганографии
7. Что такое цифровая подпись?
а) Электронный аналог обычной подписи
б) Метод шифрования данных
в) Способ подтверждения авторства документа
г) Метод аутентификации пользователя
8. Какие компоненты входят в систему сертификации?
а) Центр сертификации
б) Пользовательские сертификаты
в) Криптографические ключи
г) Все вышеперечисленное
9. Что такое криптографический протокол?
а) Набор правил для шифрования данных
б) Алгоритм работы криптосистемы
в) Набор правил и процедур для безопасного обмена информацией
г) Метод криптоанализа
10. Какой метод шифрования использует машину Энигма?
а) Симметричное шифрование
б) Асимметричное шифрование
в) Метод перестановки
г) Метод замены
11. Что такое стенография?
а) Метод шифрования
б) Метод скрытой передачи информации
в) Метод криптоанализа
г) Метод аутентификации
12. Какие недостатки имеет симметричное шифрование?
а) Низкая скорость работы
б) Сложность реализации
в) Проблема безопасного обмена ключами
г) Низкая стойкость
13. Что такое сертификат?
а) Документ, подтверждающий личность
б) Документ, подтверждающий права доступа
в) Документ, подтверждающий подлинность ключей
г) Документ, подтверждающий права собственности
14. Какой метод шифрования считается абсолютно надежным?
а) Шифр Цезаря
б) Одноразовый шифр-блокнот
в) Шифр Виженера
г) Асимметричное шифрование
15. Что такое ключ шифра?

а) Секретная информация для шифрования
б) Секретная информация для дешифрования
в) Секретная информация для обеих операций
г) Секретная информация для аутентификации

Экзамен
1. Какой нормативно-правовой акт регулирует защиту персональных данных в России?
а) ФЗ-152
б) ФЗ-98
в) ФЗ-242
г) ФЗ-352
2. Какие методы шифрования относятся к симметричным?
а) Шифр Цезаря
б) RSA
в) Шифр Виженера
г) Эллиптические кривые
3. Что относится к техническим средствам защиты персональных данных?
а) DLP-системы
б) Антивирусное ПО
в) Системы контроля доступа
г) Все вышеперечисленное
4. Какие признаки указывают на возможное заражение троянским ПО?
а) Замедление работы системы
б) Необычное поведение программ
в) Увеличение потребления ресурсов
г) Все вышеперечисленное
5. Какой метод социальной инженерии предполагает создание ложной ситуации?
а) Претекстинг
б) Фишинг
в) Тайпсвотинг
г) Квид про Кво
6. Что такое “дорожное яблоко”?
а) Метод социальной инженерии
б) Вид вредоносного ПО
в) Способ шифрования
г) Метод криптоанализа
7. Какие компоненты входят в систему цифровой подписи?
а) Открытый ключ
б) Закрытый ключ
в) Сертификат
г) Все вышеперечисленное
8. Что обеспечивает абсолютная секретность при правильном использовании?
а) Шифр Цезаря
б) Одноразовый шифр-блокнот
в) Шифр Виженера
г) Асимметричное шифрование
9. Какие характеристики должны быть у современного криптографического протокола?
а) Стойкость к атакам
б) Масштабируемость
в) Простота реализации
г) Все вышеперечисленное
10. Что относится к методам сбора информации из открытых источников?
а) Анализ социальных сетей
б) Изучение публичных баз данных
в) Мониторинг форумов
г) Все вышеперечисленное
11. Какие политики безопасности защищают от вредоносного ПО?
а) Запрет на съемные носители
б) Контроль доступа
в) Мониторинг активности
г) Все вышеперечисленное
12. Что такое атака “человек посередине”?
а) Перехват данных
б) Подмена ключей
в) Фишинг
г) Социальная инженерия
13. Какие методы защиты от фишинга являются наиболее эффективными?
а) Антиспам-фильтры
б) Проверка URL

в) Обучение персонала
г) Все вышеперечисленное
14. Что относится к категории конфиденциальной информации?
а) Персональные данные
б) Коммерческая тайна
в) Служебная тайна
г) Все вышеперечисленное
15. Какие требования предъявляются к стойким паролям?
а) Длина не менее 12 символов
б) Использование разных типов символов
в) Отсутствие словарных слов
г) Все вышеперечисленное

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	Ищейнов В.Я. Информационная безопасность и защита информации: словарь терминов и понятий [Электронный ресурс]:Словарь. - Москва: Русайнс, 2024. - 226 с. – Режим доступа: https://book.ru/book/951881
Л.1.3	Медведев В.А. Информационная безопасность. Введение в специальность + еПриложение:Тесты [Электронный ресурс]:Учебник. - Москва: КноРус, 2024. - 143 с. – Режим доступа: https://book.ru/book/951878
Л.1.4	Мельников В.П., Куприянов А.И., Васильева Т.Ю., Мельников В.П. Информационная безопасность [Электронный ресурс]:Учебник. - Москва: КноРус, 2023. - 371 с. – Режим доступа: https://book.ru/book/950148

Л.1.5	Медведев В.А. Информационная безопасность. Введение в специальность + eПриложение:Тесты [Электронный ресурс]:Учебник. - Москва: КноРус, 2023. - 143 с. – Режим доступа: https://book.ru/book/948870
Л.1.6	Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность. Лабораторный практикум + eПриложение [Электронный ресурс]:Учебное пособие. - Москва: КноРус, 2023. - 131 с. – Режим доступа: https://book.ru/book/949452
7.1.2. Дополнительная литература	
Л.2.1	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	Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition
7.2.2	Microsoft Windows 10 Pro
7.2.3	Microsoft Office 2013 Pro Plus
7.2.4	Информационно-поисковая правовая справочная система «Гарант»
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	Электронно-библиотечная система "Университетская библиотека онлайн". Режим доступа: https://biblioclub.ru/
7.3.5	Электронно-библиотечная система "Лань". Режим доступа: https://e.lanbook.com/
7.3.6	ПЛАТФОРМА ОНЛАЙН-ОБРАЗОВАНИЯ «РАЗУМ». Режим доступа: https://razoom.mgutm.ru/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1	Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1310 - Лаборатория Учебная аудитория для проведения занятий лекционного типа; занятий семинарского типа, лабораторных и практических занятий; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочие места обучающихся; Рабочее место преподавателя; Классная доска; 15 рабочих мест обучающихся оснащенные ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду; Ноутбук переносной; Переносной проектор; Переносной экран; Учебно-наглядные пособия
8.2	Адрес: 215119, Смоленская область, Вяземский район, город Вязьма, ул. Ленина, д. 77: аудитория 18-1303 - Лаборатория Учебная аудитория для проведения занятий лекционного типа; занятий семинарского типа, лабораторных и практических занятий; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочие места обучающихся; Рабочее место преподавателя; Классная доска; 11 рабочих мест обучающихся, оснащенных ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду; Комплект типового лабораторного оборудования на основе программируемого контроллера АПК1-С-К; Комплект типового лабораторного оборудования ОАП1-С-Р; макет автоматизированной системы «Умное кафе», образовательный набор по электронике, робототехнике и микропроцессорной технике.

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. пед. наук, доцент Кузьмин К.А._____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2026 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2026 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
канд. пед. наук, доцент Кузьмин К.А._____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2027 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2027 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
канд. пед. наук, доцент Кузьмин К.А._____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2028 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2028 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич _____

==========

Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы
Руководитель ОПОП
канд. пед. наук, доцент Кузьмин К.А._____

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2029 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич_____

Рабочая программа согласована на заседании выпускающей кафедры
Системной автоматизации и информационных технологий
Протокол от __ _____ 2029 г. № __
Зав. кафедрой Кузьмин Константин Анатольевич _____