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

УТВЕРЖДАЮ
Директор БИТУ (филиала)
_____ Е.В. Кузнецова
«29» мая 2024 г.

Рабочая программа дисциплины (модуля)

Б1.О.04.13 Информационная безопасность

Кафедра:	Информационные технологии и системы управления
Направление подготовки:	15.03.04 Автоматизация технологических процессов и производств
Направленность (профиль):	Эксплуатация автоматизированных систем управления
Квалификация выпускника:	Бакалавр
Форма обучения:	заочная
Год набора:	2024
Общая трудоемкость:	216 часов/6 з.е.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00940BA2D772BADC6721A08E042746B11B
Владелец: Кузнецова Елена Валентиновна
Действителен: с 07.07.2023 до 29.09.2024

Мелеуз, 2024 г.

Программу составил(и):
канд.пед.наук доц. Яшин Д.Д.

Рабочая программа дисциплины (модуля)
"Информационная безопасность"
разработана составлена на основании учебного плана, утвержденного ученым советом 28 марта 2024 г. протокол № 9 в соответствии
с ФГОС ВО Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств (приказ Минобрнауки России от 09.08.2021 г. № 730)

Руководитель ОПОП
_____ доцент, к.п.н. Одинокова Е.В.

Рабочая программа обсуждена на заседании обеспечивающей кафедры
Информационные технологии и системы управления
Протокол от 29 мая 2024 г. № 10
И.о. зав. кафедрой Одинокова Е.В._____

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цели:

Ознакомить обучающихся с правовыми основами защиты информации, организационными методами защиты информации, математическими методами, лежащими в основе защиты информации.

1.2. Задачи:

-ознакомления обучающихся с мерами и мероприятиями, обеспечивающими безопасность информации и информационных систем;
-рассмотреть основные подходы к защите информации;
-ознакомить обучающихся с наиболее широко применимыми видами технических и программных средств защиты информации.

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.

Связь с предшествующими дисциплинами (модулями), практиками

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

Распределение часов дисциплины

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

Вид промежуточной аттестации:

Экзамен 4 курс

Зачёт 4 курс

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

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

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

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

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

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

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

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

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

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

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименования разделов, тем, их краткое содержание и результаты освоения /вид занятия/	Курс	Часов	Инте ракт.	Прак. подг.	Индикаторы достижения компетенции	Оценочные средства
	Раздел 1.Основные виды и источники атак на информацию						
1.1	**Тема 1. Основные виды и источники атак на информацию** **Краткое содержание:** **1.1 Современная ситуация в области информационной безопасности;** **1.2 Категории информационной безопасности** **1.3 Абстрактные модели защиты информации** **1.4 Обзор наиболее распространенных методов "взлома"** **знать: современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования. /Лек/**	4	1	0	0	ОПК-4.1,ОПК-14.1	Тестирование Устный опрос
1.2	**Практическая работа 1. Шифрование и дешифрование файлов при помощи простейших программ** **Краткое содержание: Шифрование и дешифрование файлов при помощи простейших программ** **уметь: выбрать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты** **владеть: методами защиты информации и программного обеспечения от несанкционированного доступа и копирования**	4	1	0	0	ОПК-4.2,ОПК-4.3,ОПК-14.2,ОПК-14.3	Задания к практической работе

	/Пр/						
1.3	**Тема 1. Основные виды и источники атак на информацию** **Краткое содержание: изучить современную ситуацию в области информационной безопасности; категории информационной безопасности; абстрактные модели защиты информации, обзор наиболее распространенных методов "взлома"** **знать: современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования** **уметь: выбрать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты** **владеть: методами защиты информации и программного обеспечения от несанкционированного доступа и копирования** **/Ср/**	4	45	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	Вопросы для самоподготовки
	Раздел 2.Сетевая безопасность						
2.1	**Тема 2. Сетевая безопасность** **Краткое содержание:** **2.1 Атакуемые сетевые компоненты** **2.2 Уровни сетевых атак согласно модели OSI** **знать: устройство сетевых компонентов: сервера, рабочие станции, среда передачи информации и узлы коммутации сетей** **/Лек/**	4	1	0	0	ОПК-4.1,ОПК-14.1	Тестирование Устный опрос
2.2	**Практическая работа 2. Обжим витой пары. Соединение рабочих станций в ЛВС.** **Краткое содержание: Обжим витой пары. Соединение рабочих станций в ЛВС** **уметь: проектировать локальную сеть, объединяя сервера, рабочие станции и среду передачи информации** **владеть: навыками монтажа локальной сети.** **/Пр/**	4	1	0	0	ОПК-4.2,ОПК-4.3,ОПК-14.2,ОПК-14.3	Задания к практической работе
2.3	**Тема 2. Сетевая безопасность** **Краткое содержание: Сервера, рабочие станции, среда передачи информации и узлы коммутации сетей. Эталонная модель взаимодействия открытых систем OSI** **знать: устройство сетевых компонентов: сервера, рабочие станции, среда передачи информации и узлы коммутации сетей** **уметь: проектировать локальную сеть, объединяя сервера, рабочие станции и среду передачи**	4	46	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	Вопросы для самоподготовки

	информации **владеть: навыками монтажа локальной сети. /Ср/**						
2.4	**Зачет.** **Знать принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с 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; логику построения и принципы функционирования современных языков программирования и языков работы с базами данных, сред разработки информационных систем и технологий, принципы разработки алгоритмов и компьютерных программ; современные языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий;** **Умеет выбирать 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; выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий; читать коды**	4	4	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	Вопросы к зачету Тестирование

	программных продуктов, написанных на освоенных языках программирования, и вносить требуемые изменения; анализировать профессиональные задачи, разрабатывать подходящие информационные решения; самостоятельно осваивать новые для себя современные языки программирования и языки работы с базами данных, среды, разработки информационных систем и технологий; Владеет навыками 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; навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения; навыками отладки и тестирования прототипов программно-технических комплексов задач. **/Зачёт/**						
	Раздел 3.Криптография						
3.1	**Тема 3. Криптография Краткое содержание: 3.1 Классификация криптоалгоритмов 3.2 Симметричные криптоалгоритмы 3.3 Симметричные криптосистемы 3.4 Асимметричные криптоалгоритмы знать: классификацию криптоалгоритмов, принцип работы симметричных криптоалгоритмов и криптосистем, принцип работы асимметричных криптоалгоритмов и криптосистем. /Лек/**	4	1	0	0	ОПК-4.1,ОПК-14.1	Тестирование Устный опрос
3.2	**Практическая работа 3. Методы и средства защиты информации в Microsoft Office Краткое содержание: Методы и средства защиты информации в Microsoft Office уметь: создавать симметричные криптоалгоритмы и асимметричные криптоалгоритмы владеть: навыками зашифровки данных симметричными и асимметричными криптоалгоритмами /Пр/**	4	1	0	1	ОПК-4.2,ОПК-4.3,ОПК-14.2,ОПК-14.3	Задания к практической работе
3.3	**Лабораторная работа 1. Криптоалгоритм TEA**	4	1	0	0	ОПК-4.2,ОПК-	Отчет по лаб. работе

	Краткое содержание: Реализация криптоалгоритма TEA на языке программирования Pascal уметь: создавать симметричные криптоалгоритмы и асимметричные криптоалгоритмы владеть: навыками зашифровки данных симметричными и асимметричными криптоалгоритмами /Лаб/					4.3,ОПК-14.2,ОПК-14.3	
3.4	**Лабораторная работа 2. Криптоалгоритм Rijndael Краткое содержание: Реализация криптоалгоритма Rijndael на языке программирования Pascal уметь: создавать симметричные криптоалгоритмы и асимметричные криптоалгоритмы владеть: навыками зашифровки данных симметричными и асимметричными криптоалгоритмами /Лаб/**	4	1	0	0	ОПК-4.2,ОПК-4.3,ОПК-14.2,ОПК-14.3	Отчет по лаб. работе
3.5	**Лабораторная работа 3. Передача зашифрованного текста криптоалгоритмом Rijndael Краткое содержание: Передача зашифрованного текста криптоалгоритмом Rijndael по локальной сети на языке программирования Pascal уметь: создавать симметричные криптоалгоритмы и асимметричные криптоалгоритмы владеть: навыками зашифровки данных симметричными и асимметричными криптоалгоритмами /Лаб/**	4	2	0	0	ОПК-4.2,ОПК-4.3,ОПК-14.2,ОПК-14.3	Отчет по лаб. работе
3.6	**Лабораторная работа 4. Прием зашифрованного текста криптоалгоритмом Rijndael Краткое содержание: Прием зашифрованного текста криптоалгоритмом Rijndael по локальной сети и его расшифровка на языке программирования Pascal уметь: создавать симметричные криптоалгоритмы и асимметричные криптоалгоритмы владеть: навыками зашифровки данных симметричными и асимметричными криптоалгоритмами /Лаб/**	4	2	0	0	ОПК-4.2,ОПК-4.3,ОПК-14.2,ОПК-14.3	Отчет по лаб. работе
3.7	**Тема 3. Криптография Краткое содержание: Тайнопись, криптография с ключом, симметричные криптоалгоритмы, асимметричные криптоалгоритмы, перестановочные, подстановочные, потоковые шифры, блочные шифры знать: классификацию криптоалгоритмов, принцип работы симметричных криптоалгоритмов и криптосистем, принцип работы асимметричных криптоалгоритмов и криптосистем. уметь: создавать симметричные криптоалгоритмы и**	4	48	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	Вопросы для самоподготовки

	асимметричные криптоалгоритмы владеть: навыками зашифровки данных симметричными и асимметричными криптоалгоритмами /Ср/						
	Раздел 4.ПО и информационная безопасность. Комплексная система безопасности						
4.1	**Тема 4. ПО и информационная безопасность. Комплексная система безопасности** **Краткое содержание:** **4.1 Обзор современного ПО** **4.2 Ошибки, приводящие к возможности атак на информацию** **4.3 Основные положения по разработке ПО** **4.4 Классификация информационных объектов** **4.5 Политика ролей** **4.6 Создание политики информационной безопасности** **4.7 Методы обеспечения безотказности** **знать: информационная безопасность в операционных системах, прикладных программах, ошибки, приводящие к возможности атак на информацию, основные положения по разработке ПО, классификацию по требуемой степени безотказности, классификация по уровню конфиденциальности, требования по работе с конфиденциальной информацией,** **уметь: организовать информационную безопасность в операционных системах, прикладных программах, применять основные положения по разработке ПО, осуществлять безотказность сервисов и служб хранения данных достигается с помощью систем самотестирования и внесения избыточности на различных уровнях: аппаратном, программном, информационном** **владеть: навыками настройки информационной безопасности в операционных системах, прикладных программах, навыками применения основных положений по разработке ПО, методикой создания политики безопасности предприятия, состоящей из учета основных (наиболее опасных) рисков информационных атак.** **/Лек/**	4	1	0	0	ОПК-4.1,ОПК-14.1	Тестирование Устный опрос
4.2	**Практическая работа 4. Генерация ключей. Шифрование и расшифровка сообщений в программе PGP. Изменение парольной фразы. PGP диск. Зашифровка и расшифровка данных алгоритмом RSA. Зашифровка и расшифровка**	4	1	0	1	ОПК-4.2,ОПК-4.3,ОПК-14.2,ОПК-14.3	Задания к практической работе

	данных алгоритмом RSA Краткое содержание: Генерация ключей. Шифрование и расшифровка сообщений в программе PGP. Изменение парольной фразы. PGP диск уметь: организовать информационную безопасность в операционных системах, прикладных программах, применять основные положения по разработке ПО, осуществлять безотказность сервисов и служб хранения данных достигается с помощью систем самотестирования и внесения избыточности на различных уровнях: аппаратном, программном, информационном; организовать информационную безопасность в операционных системах, прикладных программах, применять основные положения по разработке ПО, осуществлять безотказность сервисов и служб хранения данных достигается с помощью систем самотестирования и внесения избыточности на различных уровнях: аппаратном, программном, информационном; организовать информационную безопасность в операционных системах, прикладных программах, применять основные положения по разработке ПО, осуществлять безотказность сервисов и служб хранения данных достигается с помощью систем самотестирования и внесения избыточности на различных уровнях: аппаратном, программном, информационном. владеть: навыками настройки информационной безопасности в операционных системах, прикладных программах, навыками применения основных положений по разработке ПО, методикой создания политики безопасности предприятия, состоящей из учета основных (наиболее опасных) рисков информационных атак; навыками настройки информационной безопасности в операционных системах, прикладных программах, навыками применения основных положений по разработке ПО, методикой создания политики безопасности предприятия, состоящей из учета основных (наиболее опасных) рисков информационных атак; навыками настройки информационной безопасности в операционных системах, прикладных программах, навыками применения основных положений по разработке ПО, методикой создания политики безопасности предприятия, состоящей из учета основных						

	(наиболее опасных) рисков информационных атак. /Пр/						
4.3	**Тема 4. ПО и информационная безопасность. Комплексная система безопасности** **Краткое содержание: обзор современного ПО, ошибки, приводящие к возможности атак на информацию, основные положения по разработке ПО. Классификация по требуемой степени безотказности, классификация по уровню конфиденциальности, требования по работе с конфиденциальной информацией. Рекомендуемые роли: специалист по информационной безопасности, владелец информации, поставщик аппаратного и программного обеспечения, разработчик системы и/или программного обеспечения, линейный менеджер или менеджер отдела, операторы, аудиторы.** **знать: информационная безопасность в операционных системах, прикладных программах, ошибки, приводящие к возможности атак на информацию, основные положения по разработке ПО, классификацию по требуемой степени безотказности, классификация по уровню конфиденциальности, требования по работе с конфиденциальной информацией,** **уметь: организовать информационную безопасность в операционных системах, прикладных программах, применять основные положения по разработке ПО, осуществлять безотказность сервисов и служб хранения данных достигается с помощью систем самотестирования и внесения избыточности на различных уровнях: аппаратном, программном, информационном** **владеть: навыками настройки информационной безопасности в операционных системах, прикладных программах, навыками применения основных положений по разработке ПО, методикой создания политики безопасности предприятия, состоящей из учета основных (наиболее опасных) рисков информационных атак.** **/Ср/**	4	50	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	Вопросы для самоподготовки
4.4	**Экзамен.** **Знать принципы информационной и библиографической культуры, методы и средства решения стандартных задач профессиональной деятельности с Знает процессы, методы поиска,**	4	9	0	0	ОПК-4.1,ОПК-4.2,ОПК-4.3,ОПК-14.1,ОПК-14.2,ОПК-14.3	Вопросы к экзамену Тестирование

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

	разработки информационных систем и технологий; Владеет навыками 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; навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения; навыками отладки и тестирования прототипов программно-технических комплексов задач. /Экзамен/						

Перечень применяемых активных и интерактивных образовательных технологий:

Компьютерная технология обучения

Основана на использовании информационных технологий в учебном процессе. Реализация данной технологии осуществляется посредством компьютера и иных мультимедийных средств. Использование компьютерных технологий делает учебный процесс не только современным и познавательным, но интересным для обучающихся

Технология обучения в сотрудничестве

Технология обучения в сотрудничестве используется в образовательной практике для преодоления последствий индивидуального характера учебной деятельности субъектов и их стремлений исключительно к индивидуальным образовательным достижениям. Она позволяет обогатить опыт и приобрести через учебный труд те навыки совместимой деятельности, которые затем могут стать необходимыми в будущей профессиональной и социальной деятельности в течение жизни. Цель технологии состоит в формировании умений у субъектов образовательного процесса эффективно работать сообща во временных командах и группах и добиваться качественных образовательных результатов

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

СРС – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (возможно частичное непосредственное участие преподавателя при сохранении ведущей роли студентов). Целью СРС является овладение фундаментальными знаниями, профессиональными умениями и навыками по профилю будущей специальности, опытом творческой, исследовательской деятельности, развитие самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровней. Задачи СРС: систематизация и закрепление полученных теоретических знаний и практических умений студентов; углубление и расширение теоретической подготовки; формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу; развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности; формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации; развитие исследовательских умений; использование материала, собранного и полученного в ходе самостоятельных занятий на практических занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам. Функции СРС: развивающая (повышение культуры умственного труда, приобщение к 10 творческим видам деятельности, обогащение интеллектуальных способностей студентов); информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится мало результативной); ориентирующая и стимулирующая (процессу обучения придается ускорение и мотивация); воспитательная (формируются и развиваются профессиональные качества специалиста и гражданина); исследовательская (новый уровень профессионально-творческого мышления).

Самостоятельная работа студентов является обязательным компонентом учебного процесса для каждого студента и определяется учебным планом. Виды самостоятельной работы студентов определяются при разработке рабочих программ и учебных методических комплексов дисциплин содержанием учебной дисциплины. При определении содержания самостоятельной работы студентов следует учитывать их уровень самостоятельности и требования к уровню самостоятельности выпускников для того, чтобы за период обучения искомый уровень был достигнут. Так, удельный вес самостоятельной работы при обучении в очной форме составляет до 50% от количества аудиторных часов, отведённых на изучение дисциплины, в заочной форме - количество часов, отведенных на освоение дисциплины, увеличивается до 90%. Самостоятельная работа определяется как индивидуальная или коллективная учебная деятельность, осуществляемая без непосредственного руководства педагога, но по его заданиям и под его контролем. Самостоятельная работа – это

познавательная учебная деятельность, когда последовательность мышления студента, его умственных и практических операций и действий зависит и определяется самим студентом.
Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня, что в итоге приводит к развитию навыка самостоятельного планирования и реализации деятельности. Целью самостоятельной работы студентов является овладение необходимыми компетенциями по своему направлению подготовки, опытом творческой и исследовательской деятельности.
На основании компетентностного подхода к реализации профессиональных образовательных программ, видами заданий для самостоятельной работы являются:
- для овладения знаниями: чтение текста (учебника, первоисточника, дополнительной литературы), составление плана текста, графическое изображение структуры текста, конспектирование текста, выписки из текста, работа со словарями и справочниками, ознакомление с нормативными документами, учебно-исследовательская работа, использование аудио- и видеозаписей, компьютерной техники и информационно-телекоммуникационной сети Интернет и др.
- для закрепления и систематизации знаний: работа с конспектом лекции, обработка текста (учебника, первоисточника, дополнительной литературы, аудио и видеозаписей), повторная работа над учебным материалом, составление плана, составление таблиц для систематизации учебного материала, ответ на контрольные вопросы, заполнение рабочей тетради, аналитическая обработка текста (аннотирование, рецензирование, реферирование, конспект-анализ и др.), завершение аудиторных практических работ и оформление отчётов по ним, подготовка мультимедиа сообщений/докладов к выступлению на семинаре (конференции), материалов-презентаций, подготовка реферата, составление библиографии, тематических кроссвордов, тестирование и др.
- для формирования умений: решение задач и упражнений по образцу, решение вариативных задач, выполнение чертежей, схем, выполнение расчетов (графических работ), решение ситуационных (профессиональных) задач, подготовка к деловым играм, проектирование и моделирование разных видов и компонентов профессиональной деятельности, рефлексивный анализ профессиональных умений с использованием аудио- и видеотехники и др.
Самостоятельная работа может осуществляться индивидуально или группами студентов в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений студентов.

6. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

6.1. Перечень компетенций с указанием этапов формирования индикаторов их достижения в процессе освоения ОПОП

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

Недостаточный уровень:

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

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

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

Пороговый уровень:

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

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

Владеет навыками разработки оригинальных алгоритмов пригодных для практического применения

Продвинутый уровень:

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

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

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

Высокий уровень:

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

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

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

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

Недостаточный уровень:

Не 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

Не 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

Не 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

Пороговый уровень:

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

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

Владеет навыками работы с данными с помощью информационных технологий;

Продвинутый уровень:

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

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

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

Высокий уровень:

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

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

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

6.2. 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; - 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.	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания, которые следует выполнить.	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала; -способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; - 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.	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
0 - 59 баллов	**60 - 69 баллов**	**70 - 89 баллов**	**90 - 100 баллов**
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
Не 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
Не умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки

оригинальных алгоритмов и компьютерных программ, пригодных для практического применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий; читать коды программных продуктов, написанных на освоенных языках программирования, и вносить требуемые изменения; анализировать профессиональные задачи, разрабатывать подходящие информационные решения; самостоятельно осваивать новые для себя современные языки программирования и языки работы с базами данных, среды, разработки информационных систем и технологий
Не знает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); логику построения и принципы функционирования современных языков программирования и языков работы с базами данных, сред разработки информационных систем и технологий, принципы разработки алгоритмов и компьютерных программ; современные языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий
Не 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
Не 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
Не владеет навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения; навыками отладки и тестирования прототипов программно-технических комплексов задач
2. Пороговый уровень
Знает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии)
Умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач
Владеет навыками работы с данными с помощью информационных технологий;
Умеет выбирать и использовать современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы и программные средства
Владеет навыками разработки оригинальных алгоритмов пригодных для практического применения
Знает процессы, методы поиска, сбора, хранения, обработки, представления, распространения информации и способы осуществления таких процессов и методов (информационные технологии)
3. Продвинутый уровень
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
Владеет навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения
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
Знает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); логику построения и принципы функционирования современных языков программирования и языков работы с базами данных, сред разработки информационных систем и технологий, принципы разработки алгоритмов и компьютерных программ
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
Умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий
4. Высокий уровень
Умеет выбирать языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий, исходя из имеющихся задач; применять современные языки программирования для разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения, вести базы данных и информационные хранилища, применять современные программные среды разработки информационных систем и технологий; читать коды программных продуктов, написанных на освоенных языках программирования, и вносить требуемые изменения; анализировать профессиональные задачи, разрабатывать подходящие информационные решения; самостоятельно осваивать новые для себя современные языки программирования и языки работы с базами данных, среды, разработки информационных систем и технологий
Владеет навыками 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
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
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
Знает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (информационные технологии); логику построения и принципы функционирования современных языков программирования и языков работы с базами данных, сред разработки информационных систем и технологий, принципы разработки алгоритмов и компьютерных программ; современные языки программирования и языки работы с базами данных, среды разработки информационных систем и технологий
Владеет навыками разработки оригинальных алгоритмов и компьютерных программ, пригодных для практического применения; навыками отладки и тестирования прототипов программно-технических комплексов задач

В случае, если сумма рейтинговых баллов, полученных при прохождении промежуточной аттестации составляет от 0 до 9 баллов, то зачет/ зачет с оценкой/ экзамен НЕ СДАН, независимо от итогового рейтинга по дисциплине.
В случае, если сумма рейтинговых баллов, полученных при прохождении промежуточной аттестации находится в пределах от 10 до 30 баллов, то зачет/ зачет с оценкой/ экзамен СДАН, и результат сдачи определяется в зависимости от итогового рейтинга по дисциплине в соответствии с утвержденной шкалой перевода из 100-балльной шкалы оценивания в 5-балльную.
Для приведения рейтинговой оценки по дисциплине по 100-балльной шкале к аттестационной по 5-балльной шкале в соответствии с Положением о балльно-рейтинговой системе оценки успеваемости студентов федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет технологий и управления имени К.Г. Разумовского (Первый казачий университет) используется следующая шкала:

Аттестационная оценка по дисциплине	Рейтинговая оценка по дисциплине
"ОТЛИЧНО"	90 - 100 баллов
"ХОРОШО"	70 - 89 баллов
"УДОВЛЕТВОРИТЕЛЬНО"	60 - 69 баллов
"НЕУДОВЛЕТВОРИТЕЛЬНО"	менее 60 баллов
"ЗАЧТЕНО"	более 60 баллов
"НЕ ЗАЧТЕНО"	менее 60 баллов

6.3. Оценочные средства текущего контроля (примерные темы докладов, рефератов, эссе)
Вопросы для устного опроса
Тема 1. Основные виды и источники атак на информацию
1. Аргументируйте прогресс информационных технологий и необходимость обеспечения информационной безопасности.
2. Раскройте основные понятия информационной безопасности.
3. Система защиты информации и ее структура.
4. Рассмотрите экономическую информацию, как товар и объект безопасности.
5. Приведите профессиональные тайны, их виды.
6. Расскажите про персональные данные и их защиту.
7. Раскройте информационные угрозы, их виды и причины возникновения.
8. Приведите информационные угрозы для государства.
9. Приведите информационные угрозы для компании.
10. Приведите информационные угрозы для личности (физического лица).

Тема 2. Сетевая безопасность
1. Опишите защиту информации в Интернете.
2. Опишите защита электронной почты.
3. Опишите защиту от компьютерных вирусов.
5. Рассмотрите популярные антивирусные программы и их классификацию.
6. Приведите примеры организации системы защиты информации экономических объектов
7. Рассмотрите атакуемые сетевые компоненты
8. Приведите уровни сетевых атак согласно модели OSI
9. Раскройте особенности защиты информации в серверах
10. Раскройте особенности защиты информации в рабочих станциях

Тема 3. Криптография
1. Приведите классификацию криптоалгоритмов
2. Приведите принцип работы симметричных криптоалгоритмов
3. Приведите принцип работы симметричных криптосистем
4. Приведите принцип работы асимметричных криптоалгоритмов
5. Приведите принцип работы асимметричных криптосистем

6. Опишите методы и средства защиты информации в Microsoft Office
7. Опишите принцип работы криптоалгоритма TEA
8. Опишите принцип работы криптоалгоритма Rijndael
9. Раскройте особенности передачи зашифрованного текста криптоалгоритмом Rijndael
10. Назовите отличия тайнописи от криптографии с ключом,

Тема 4. ПО и информационная безопасность. Комплексная система безопасности
1. Опишите политика безопасности и ее принципы.
2. Раскройте фрагментарный и системный подход к защите информации.
3. Опишите методы защиты информации.
4. Опишите средства защиты информации.
5. Раскройте организационное обеспечение ИБ.
6. Рассмотрите организацию конфиденциального делопроизводства.
7. Назовите комплекс организационно-технических мероприятий по обеспечению защиты информации.
8. В чем заключается инженерно-техническое обеспечение компьютерной безопасности?
9. Приведите план обеспечения непрерывной работы и восстановления функционирования автоматизированной информационной системы.
10. В чем заключается управление информационной безопасности на государственном уровне?

Вопросы для самоподготовки:
Тема 1. Основные виды и источники атак на информацию
1. Приведите объекты коммерческой тайны на предприятии.
2. Раскройте современную ситуацию в области информационной безопасности;
3. Назовите категории информационной безопасности в отношении информации
4. Назовите категории информационной безопасности в отношении информационных систем
5. Приведите абстрактные модели защиты информации
6. Приведите обзор наиболее распространенных методов "взлома"
7. Раскройте способы получение пароля на основе ошибок администратора
8. Раскройте способы получение пароля на основе ошибок пользователей
9. Опишите терминалы защищенной информационной системы
10. Опишите социальную психологию и иные способы получения паролей

Тема 2. Сетевая безопасность
1. Опишите основные атаки на DNS-сервера
2. Опишите особенности атак на широковещательные линии с неограниченным доступом
3. Опишите особенности атак на широковещательные линии с ограниченным доступом
4. Опишите особенности атак на каналы "точка-точка"
5. В чем заключаются особенности прослушивания сетевого трафика в не витой паре?
6. В чем заключаются особенности прослушивания сетевого трафика в витой паре?
7. В чем заключаются особенности прослушивания сетевого трафика в коаксиальном проводе?
8. В чем заключаются особенности прослушивания сетевого трафика в оптическом волокне?
9. Опишите особенности обжима витой пары.
10. Опишите особенности соединения рабочих станций в ЛВС

Тема 3. Криптография
1. Назовите особенности перестановочных криптоалгоритмов
2. Назовите особенности подстановочных криптоалгоритмов
3. Назовите особенности потоковых шифров
4. Назовите особенности блочных шифров
5. В чем заключается принцип работы сети Фейштеля?
6. В чем заключается принцип работы скремблеров?
7. Опишите принцип работы криптоалгоритма RSA
8. Назовите особенности хеширования паролей
9. Назовите функции криптосистем
10. В чем заключается транспортное кодирование?

Тема 4. ПО и информационная безопасность. Комплексная система безопасности.
1. В чем заключается защита электронной коммерции?
2. Менеджмент и аудит информационной безопасности на уровне предприятия.
3. Информационная безопасность предпринимательской деятельности. Аудит ИБ автоматизированных банковских систем.
4. Рассмотрите обзор современного ПО
5. Опишите ошибки, приводящие к возможности атак на информацию
6. Назовите основные положения по разработке ПО
7. Приведите классификацию информационных объектов
8. В чем заключается политика ролей?
9. Опишите процесс создания политики информационной безопасности
10. Назовите методы обеспечения безотказности

Задания для практических работ
Практическая работа 1. Шифрование и дешифрование файлов при помощи простейших программ

1. Зашифруйте и расшифруйте текстовый файл программой Codefile
2. Зашифруйте и расшифруйте текстовый файл программой CryptoFan 2
3. Зашифруйте и расшифруйте текстовый файл программой DX Secure 4.0
4. Зашифруйте и расшифруйте текстовый файл программой Visual AES 1.1
5. Зашифруйте и расшифруйте текстовый файл при помощи алгоритма шифрования CFB и OFB программы Visual AES 1.1.

Практическая работа 2. Обжим витой пары. Соединение рабочих станций в ЛВС.
1 Произведите обжим двух проводов витой пары с коннектором RG45 для подключения компьютеров в ЛВС через концентратор или коммутатор
2 Соедините компьютеры через концентратор или коммутатор
3 Проверьте пропускную способность полученной ЛВС утилитой ping
4 Произведите обжим одного провода витой пары с коннектором RG45 для подключения двух компьютеров друг к другу
5 Проверьте пропускную способность полученной ЛВС утилитой ping

Практическая работа 3. Методы и средства защиты информации в Microsoft Office
1 Установите пароль на открытие файла в MS Word.
2 Установите ограничения на форматирование в MS Word.
3 Установите ограничения на редактирование в MS Word.
4 Установите пароль на открытие файла в MS Excel.
5 Установите защиту листа в MS Excel.
6 Установите защиту книги в MS Excel.

Практическая работа 4. Генерация ключей. Шифрование и расшифровка сообщений в программе PGP. Изменение парольной фразы. PGP диск. Зашифровка и расшифровка данных алгоритмом RSA.
1 Сгенерируйте ключи в программе PGP.
2 Создайте парольную фразу к закрытому ключу
3 Сохраните ключи и произведите обмен открытых ключей
4 Зашифруйте текстовый файл чужим открытым ключом и отправьте владельцу
5 Расшифруйте закрытым ключом, полученный зашифрованный файл.
6 Измените парольную фразу
7 Создайте PGP диск
8 Установите пароль на PGP диск
9 Переместите файлы на PGP диск и скройте его
10 Восстановите доступ к PGP диску
11 Выберете простые числа p и q
12 Вычислите в MS Excel n = p * q
13 Вычислите в MS Excel f(n) = (p - 1) * (q - 1)
14 Выберете число d взаимно простое с f(n), т.е. НОД (d, f(n))=1, 1<d<= f(n).
15 Выберете число e так, чтобы e*d mod f(n) =1, e<n.

Задания для лабораторных работ
Лабораторная работа 1. Криптоалгоритм TEA
1. Написать программу шифрования, используя криптоалгоритм TEA на языке программирования Pascal
2. Написать процедуру дешифровки DeCryptRouting на языке программирования Pascal.
3. Написать программу шифрования и дешифровки одновременно.
4. Написать основную программу: ввод строковой переменной; вызов процедуры EnCryptRouting, в качестве параметра которой строковая переменная; вывод строковой переменной; вызов процедуры DeCryptRouting, в качестве параметра которой строковая переменная; вывод строковой переменной.
5. Реализовать криптоалгоритм TEA в среде программирования Visual Basic.

Лабораторная работа 2. Криптоалгоритм Rijndael
1. Разработать алгоритм ключа шифрования криптоалгоритмом Rijndael
2. Написать программу шифрования, используя криптоалгоритм Rijndael на языке программирования Pascal.
3. Разработать алгоритм ключа дешифровки криптоалгоритмом Rijndael
4. Написать программу шифрования и дешифровки одновременно на языке программирования Pascal.
4. Реализовать криптоалгоритм Rijndael в среде программирования Visual Basic.

Лабораторная работа 3. Передача зашифрованного текста криптоалгоритмом Rijndael
1. Разработать алгоритм записи текста в текстовый файл.
2. Написать программу шифрования, используя криптоалгоритм Rijndael и осуществить запись зашифрованного текста в текстовый файл.
3. Передать средствами ЛВС зашифрованный файл на соседний компьютер.
4. Реализовать передачу на другой компьютер криптоалгоритма Rijndael в среде программирования Visual Basic.

Лабораторная работа 4. Прием зашифрованного текста криптоалгоритмом Rijndael
1. Разработать алгоритм чтения текста из текстового файла.
2. Написать программу дешифровки, используя криптоалгоритм Rijndael на языке программирования Pascal и осуществить чтение зашифрованного текста из текстового файла в одномерный массив, который затем необходимо расшифровать.

аутентичность
апеллируемость

2. Гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения
конфиденциальность
целостность
аутентичность
апеллируемость

3. Гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется фальсификацией, но уже автора сообщения
конфиденциальность
целостность
аутентичность
апеллируемость

4. Гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой; отличие этой категории от предыдущей в том, что при подмене автора, кто-то другой пытается заявить, что он автор сообщения, а при нарушении апеллируемости – сам автор пытается "откреститься" от своих слов, подписанных им однажды.
конфиденциальность
целостность
аутентичность
апеллируемость

5. Гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано
надежность
точность
контроль доступа
контролируемость

6. Гарантия точного и полного выполнения всех команд
надежность
точность
контроль доступа
контролируемость

7. Гарантия того, что различные группы лиц имеют различный доступ к информационным объектам, и эти ограничения доступа постоянно выполняются
надежность
точность
контроль доступа
контролируемость

8. Гарантия того, что в любой момент может быть произведена полноценная проверка любого компонента программного комплекса
устойчивость к умышленным сбоям
контроль идентификации
контроль доступа
контролируемость

9. Гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает
устойчивость к умышленным сбоям
контроль идентификации
контроль доступа
контролируемость

10. Гарантия того, что при умышленном внесении ошибок в пределах заранее оговоренных норм система будет вести себя так, как оговорено заранее.
устойчивость к умышленным сбоям
контроль идентификации
контроль доступа
контролируемость

Тема 2. Сетевая безопасность
1. Троянская программа, троянец -
1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.
2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.
5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

3. Уровень модели OSI, который отвечает за преобразование электронных сигналов в сигналы среды передачи информации (импульсы напряжения, радиоволны, инфракрасные сигналы). На этом уровне основным классом атак является "отказ в сервисе". Постановка шумов по всей полосе пропускания канала может привести к "надежному" разрыву связи.
Физический уровень
Канальный уровень
Сетевой уровень
Транспортный уровень
Сеансовый уровень

4. Уровень модели OSI, который управляет синхронизацией двух и большего количества сетевых адаптеров, подключенных к единой среде передачи данных. Примером его является протокол EtherNet.
Физический уровень
Канальный уровень
Сетевой уровень
Транспортный уровень
Сеансовый уровень

5. Уровень модели OSI, который отвечает за систему уникальных имен и доставку пакетов по этому имени, то есть за маршрутизацию пакетов. Примером такого протокола является протокол Интернета IP.
Физический уровень
Канальный уровень
Сетевой уровень
Транспортный уровень
Сеансовый уровень

6 Уровень модели OSI, который отвечает за доставку больших сообщений по линиям с коммутацией пакетов. Так как в подобных линиях размер пакета представляет собой обычно небольшое число (от 500 байт до 5 килобайт), то для передачи больших объемов информации их необходимо разбивать на передающей стороне и собирать на приемной.
Физический уровень
Канальный уровень
Сетевой уровень
Транспортный уровень
Сеансовый уровень

7. Уровень модели OSI, который отвечает за процедуру установления начала сеанса и подтверждение (квитирование) прихода каждого пакета от отправителя получателю.
Физический уровень
Канальный уровень
Сетевой уровень
Транспортный уровень
Сеансовый уровень

8. Непредусмотренное взаимодействие данных между собой и данных с кодом
Интерференция
Нарушение неявных ограничений
Нет верного ответа

9. Какая утилита позволяет определить настройки компьютера для подключения к локальной сети и к сети Internet
Ipconfig
ping
tracert
Whois

10. При помощи какой утилиты возможно исследование топологии фрагментов сети Internet
Ipconfig
ping
tracert
Whois

Тема 3. Криптография
1. Для зашифровки и расшифровки сообщения используется один и тот же блок информации (ключ)
Симметричные криптоалгоритмы
Асимметричные криптоалгоритмы
Тайнопись
Нет верного ответа

Симметричные криптоалгоритмы
Асимметричные криптоалгоритмы
Тайнопись
Нет верного ответа

4. В зависимости от характера воздействий, производимых над данными, алгоритмы подразделяются на
Перестановочные и подстановочные
Симметричные криптоалгоритмы и асимметричные криптоалгоритмы
Потоковые и блочные
Нет верного ответа

5. Метод обратимых преобразований текста, при котором значение, вычисленное от одной из частей текста, накладывается на другие части.
Сеть Фейштеля
Скремблеры
Симметричные криптоалгоритмы и асимметричные криптоалгоритмы
Потоковые криптоалгоритмы
Нет верного ответа

6. В зависимости от размера блока информации криптоалгоритмы делятся на:
Перестановочные и подстановочные
Симметричные криптоалгоритмы и асимметричные криптоалгоритмы
Потоковые и блочные
Нет верного ответа

7. Алгоритм сжатия ориентирован на неосмысленные последовательности символов какого-либо алфавита.
Алгоритм Хаффмана
Алгоритм Лемпеля-Зива
Алгоритм Rijndael
Алгоритм TEA

8. Алгоритм сжатия основан наоборот на корреляциях между расположенными рядом символами алфавита (словами, управляющими последовательностями, заголовками файлов фиксированной структуры)
Алгоритм Хаффмана
Алгоритм Лемпеля-Зива
Алгоритм Rijndael
Алгоритм TEA

9. В каком криптоалгоритме единицей кодирования является один бит?
Потоковые шифры
Блочные шифры
Подстановочные криптоалгоритмы
Перестановочные криптоалгоритмы

10. В каком криптоалгоритме единицей кодирования является блок из нескольких байтов?
Потоковые шифры
Блочные шифры
Подстановочные криптоалгоритмы
Перестановочные криптоалгоритмы

Тема 4. ПО и информационная безопасность. Комплексная система безопасности
1. Лицо, непосредственно работающее с данной информацией. Зачастую только он в состоянии реально оценить класс обрабатываемой информации, а иногда и рассказать о нестандартных методах атак на нее (узкоспецифичных для этого вида данных).
Специалист по информационной безопасности
Владелец информации
Поставщик аппаратного и программного обеспечения
Линейный менеджер

2. Обычно стороннее лицо, которое несет ответственность перед фирмой за поддержание должного уровня информационной безопасности в поставляемых им продуктов.
Специалист по информационной безопасности
Владелец информации
Поставщик аппаратного и программного обеспечения
Линейный менеджер

3. Лицо, которое является промежуточным звеном между операторами и специалистами по информационной безопасности. Его задача – своевременно и качественно инструктировать подчиненный ему персонал обо всех требованиях службы безопасности и следить за ее их выполнением на рабочих местах.
Специалист по информационной безопасности
Владелец информации

Владелец информации
Оператор
Линейный менеджер

5. Внешние специалисты или фирмы, нанимаемые предприятием для периодической (довольно редкой) проверки организации и функционирования всей системы безопасности
Специалист по информационной безопасности
Владелец информации
Оператор
Аудиторы

6. Лицо, которое проводит расчет и перерасчет рисков, ответственен за поиск самой свежей информации об обнаруженных уязвимостях в используемом в фирме программном обеспечении и в целом в стандартных алгоритмах
Специалист по информационной безопасности
Владелец информации
Оператор
Линейный менеджер

7. Максимально возможное непрерывное время отказа для информации 0 класса безотказности
1 неделя
1 сутки
1 час
20 минут

8. Максимально возможное непрерывное время отказа для информации 1 класса безотказности
1 неделя
1 сутки
1 час
20 минут

9. Максимально возможное непрерывное время отказа для информации 2 класса безотказности
1 неделя
1 сутки
1 час
20 минут

10. Максимально возможное непрерывное время отказа для информации 3 класса безотказности
1 неделя
1 сутки
1 час

6.4. Оценочные средства промежуточной аттестации.

Вопросы к зачету:
(Компетенция ОПК-4)

Вопросы для проверки уровня обученности "знать":
1. Раскройте понятие «конфиденциальность»
2. Раскройте понятие «целостность»
3. Раскройте понятие «аутентичность»
4. Раскройте понятие «апеллируемость»
5. Раскройте понятие «надежность»
6. Раскройте понятие «точность»
7. Раскройте понятие «контроль доступа»
8. Раскройте понятие «контролируемость»
9. В чем заключается контроль идентификации?
10. Что представляет собой троянская программа?
11. Что должен запрашивать любой удаленный терминал?
12. Какое предупреждение рекомендуется выводить на экран на входе в информационную систему?
13. Как должен подбираться пароль для входа в информационную систему?
14. Что должно происходить в момент отправки пакета подтверждения или отвержения пароля?
15. Что необходимо сделать с паролями по умолчанию?

Вопросы для проверки уровня обученности "уметь":
1. В чем заключается комплексный поиск возможных методов доступа?
2. Что должно происходить с паролями через определенные промежутки времени?
3. Что должно происходить с неиспользуемыми в течение долгого времени именами регистрации?
4. Как должна реагировать система на ошибочные попытки войти в систему?
5. Назовите основные 4 возможные цели злоумышленников при атаке на сервер
6. Назовите основную целью атаки на рабочую станцию

7. Назовите основное средство атаки на рабочую станцию с целью получения данных, обрабатываемых, либо локально хранимых на ней
8. Назовите категорию схемы передачи информации, возможность считывания информации с которых ничем не контролируется
9. Опишите особенности прослушивания сетевого трафика при передаче по коаксиальному проводу
10. Опишите особенности прослушивания сетевого трафика при передаче по оптическому волокну
11. Опишите последовательность цветов проводов витой пары при прямом обжиме, который применяется для передачи данных компьютер – коммутатор – компьютер
12. Опишите последовательность цветов проводов витой пары при перекрестном обжиме, который применяется для передачи данных компьютер – компьютер
13. Назовите предназначение утилиты Ipconfig
14. Назовите предназначение утилиты tracert
15. Назовите предназначение утилиты ping

Вопросы для проверки уровня обученности "владеть":
1. С помощью утилиты ipconfig определить IP адрес и физический адрес основного сетевого интерфейса компьютера, IP адрес шлюза, IP адреса DNS-серверов и используется ли DHCP.
2. Установите пароль на открытие файла в MS Word
3. Установите ограничение на форматирование текста установкой пароля в MS Word
4. Установите ограничение на редактирование текста установкой пароля в MS Word
5. Установите пароль на открытие файла в MS Excel
6. Установить защиту листа в MS Excel.
7. Установить защиту книги в MS Excel
8. Защитите все ячейки листа кроме одной.
9. Защитите один столбец листа.
10. Защитите только одну ячейку листа.
11. Вставьте изображение на лист и защитите только его
12. Зашифруйте текстовый файл программой Visual AES 1.1
13. Зашифруйте текстовый файл программой DX Secure 4.0
14. Зашифруйте текстовый файл программой CryptoFan 2
15. Зашифруйте текстовый файл программой Codefile

(Компетенция ОПК-14)
Вопросы для проверки уровня обученности "знать":

1. В каких случаях могут использовать терминалы без пароля?
2. В каких случаях имеется обязательное требование наличия у терминала имя регистрации и пароля?
3. Назовите основное требование к удаленному терминалу
4. В чем заключается схема обратного звонка?
5. Назовите требования, предъявляемые к log-in запросу терминала
6. Что рекомендуется выводить на экран на входе в систему?
7. Назовите понятие, в котором дается гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется хищением либо раскрытием информации
8. Назовите понятие, в котором дается гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений; нарушение этой категории называется фальсификацией сообщения
9. Назовите понятие, в котором дается гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор; нарушение этой категории также называется фальсификацией, но уже автора сообщения
10. Назовите понятие, в котором дается гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой; отличие этой категории от предыдущей в том, что при подмене автора, кто-то другой пытается заявить, что он автор сообщения, а при нарушении апеллируемости – сам автор пытается "откреститься" от своих слов, подписанных им однажды.
11. Назовите понятие, в котором дается гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано
12. Назовите понятие, в котором дается гарантия точного и полного выполнения всех команд
13. Назовите понятие, в котором дается гарантия того, что различные группы лиц имеют различный доступ к информационным объектам, и эти ограничения доступа постоянно выполняются
14. Назовите понятие, в котором дается гарантия того, что в любой момент может быть произведена полноценная проверка любого компонента программного комплекса
15. Назовите понятие, в котором дается гарантия того, что клиент, подключенный в данный момент к системе, является именно тем, за кого себя выдает

Вопросы для проверки уровня обученности "уметь":
1. В чем заключается комплексная защита от возможности кражи паролей
2. Назовите основную рекомендацию при проектировании топологии сети
3. Опишите оптимальную единицу сегментирования сети
4. В чем заключается обязательное требование для операторов с разными уровнями доступа
5. Что представляет собой атака на сервер, которая вызывает "отказ в сервисе"?
6. Опишите особенность атак на DNS-сервера
7. Опишите основой класс атак на физическом уровне модели OSI
8. Опишите основой класс атак на канальном уровне модели OSI

6. Расшифруйте текстовый файл программой DX Secure 4.0
7. Зашифруйте текстовый файл программой CryptoFan 2
8. Расшифруйте текстовый файл программой CryptoFan 2
9. Зашифруйте текстовый файл программой Codefile
10. Расшифруйте текстовый файл программой Codefile
11. Защитите структуру книги в Excel
12. Защите окно книги в Excel
13. Настройте открытие презентации PowerPoint только для чтения
14. Установите пароль на открытие файла в MS PowerPoint
15. Настройте открытие документа в MS Word только для чтения

Вопросы к экзамену:
(Компетенция ОПК-4)

Вопросы для проверки уровня обученности "знать":
1. Опишите особенность работы симметричного криптоалгоритма
2. Опишите принцип работы асимметричного криптоалгоритма
3. Что подразумевает тайнопись?
4. Что представляет собой сеть Фейштеля?
5. Опишите Алгоритм Хаффмана
6. Опишите Лемпеля-Зива
7. В каком криптоалгоритме единицей кодирования является один бит?
8. На какие два вида делятся криптоалгоритмы в зависимости от размера шифруемого блока информации?
9. Дайте определение скремблера
10. К какому типу алгоритма относится шифр Rijndael?
11. Назовите три основные функции криптосистем
12. Назовите две основные методики внесения случайности в процесс шифрования
13. Назовите две большие группы алгоритмов архивации
14. Назовите и опишите два основных метода архивации без потерь
15. Что подразумевает Хеширование паролей?

Вопросы для проверки уровня обученности "уметь":
1. Опишите функции специалиста по информационной безопасности на предприятии
2. Назовите лицо, непосредственно работающее с информацией. Зачастую только он в состоянии реально оценить класс обрабатываемой информации, а иногда и рассказать о нестандартных методах атак на нее (узкоспецифичных для этого вида данных)
3. Назовите роль, которую выполняет обычно стороннее лицо, которое несет ответственность перед фирмой за поддержание должного уровня информационной безопасности в поставляемых им продуктов
4. В чем заключается роль линейного менеджера?
5. Назовите роль, которую выполняют лица, ответственные только за свои поступки. Они не принимают никаких решений и ни за кем не наблюдают
6. В чем заключается роль аудитора в организации политики информационной безопасности?
7. Напишите формулу зашифровки буквы кодируемого сообщения в алгоритме RSA и объясните ее
8. Напишите формулу зашифровки буквы кодируемого сообщения в алгоритме RSA и объясните ее
9. Напишите формулу расчета открытого ключа в алгоритме RSA и объясните ее, а также какие ограничения накладываются на открытый ключ при его нахождении.
10. Напишите формулу расчета закрытого ключа в алгоритме RSA и объясните ее, а также какие ограничения накладываются на открытый ключ при его нахождении.
11. Назовите особенность зашифровки в перестановочном алгоритме
12. Опишите основной принцип работы скремблера
13. Опишите характерную особенность блочных криптоалгоритмов
14. Дайте определение криптосистеме
15. Перечислите основные функции криптосистем

Вопросы для проверки уровня обученности "владеть":
1. Рассчитайте значение закрытого ключа в криптоалгоритме RSA, если параметры шифрования p=3 и q=11
2. Рассчитайте значение открытого ключа в криптоалгоритме RSA, если параметры шифрования p=3 и q=11, закрытый ключ d=3
3. Зашифруйте криптоалгоритмом RSA букву Б, которой соответствует значение 2, если параметры шифрования p=3 и q=11
4. Расшифруйте криптоалгоритмом RSA зашифрованную букву, значение которой 29, если параметры шифрования p=3 и q=11
5. Напишите процедуру зашифровки криптоалгоритма TEA на языке программирования Pascal
6. Напишите алгоритм создания основной программы по вызову процедуры зашифровки текста криптоалгоритмом TEA, передачи процедуре исходного текста и вывода зашифрованного.
7. Напишите на языке программирования Pascal основную программу по вызову процедуры зашифровки текста криптоалгоритмом TEA, передачи процедуре исходного текста и вывода зашифрованного.
8. Реализуйте на языке программирования Pascal зашифровку текста криптоалгоритмом TEA
9. Напишите алгоритм изменения процедуры зашифровки EnCryptRouting на процедуру расшифровки DeCryptRouting
10. Напишите фрагмент программы на Pascal, в котором для алгоритма Rijndael происходит преобразование текста,

2. Назовите основную логическую операцию, используемую в Скремблерах
3. Что подразумевает собой кодирующий поток в скремблерах?
4. Назовите существенный недостаток скремблирующих алгоритмов
5. Назовите характерную особенность блочных криптоалгоритмов
6. Опишите понятие «ветви сети Фейштеля»
7. Какие характеристики сети Фейштеля используются в криптоалгоритме – TEA?
8. Опишите основной недостаток криптоалгоритма TEA
9. В чем заключается транспортное кодирование?
10. В чем заключается первый этап любого асимметричного алгоритма?
11. Какую проблему информационной безопасности позволяет решать асимметричное шифрования?
12. Дайте определение криптосистемы
13. В чем заключается метод шифрования ECB?
14. Назовите три основные способа введение какой-либо случайной величины в процесс шифрования
15. В чем заключается проблема всех методов рандомизации сообщений?

Вопросы для проверки уровня обученности "уметь":
1. Какого одного из самых главных недостатков лишены асимметричные криптосистемы по отношению к симметричным алгоритмам
2. В каком случае троянская программа с вероятностью 90% не будет обнаружена стандартным антивирусным ПО?
3. Каким образом можно обнаруживать троянские программы, которые постоянно обеспечивают доступ к зараженной ЭВМ, с помощью утилит контроля за сетевыми портами
4. Какой утилитой для операционных систем клона Microsoft Windows можно обнаружить троянские программы
5. В чем заключаются атаки с целью изменения таблицы маршрутизации?
6. Назовите максимально возможное непрерывное время отказа для информации 0 класса безотказности
7. Назовите максимально возможное непрерывное время отказа для информации 1 класса безотказности
8. Назовите максимально возможное непрерывное время отказа для информации 2 класса безотказности
9. Назовите максимально возможное непрерывное время отказа для информации 3 класса безотказности
10. Назовите обычно стороннее лицо, которое несет ответственность перед фирмой за поддержание должного уровня информационной безопасности в поставляемых им продуктов.
11. Назовите лицо, которое является промежуточным звеном между операторами и специалистами по информационной безопасности. Его задача – своевременно и качественно инструктировать подчиненный ему персонал обо всех требованиях службы безопасности и следить за ее их выполнением на рабочих местах.
12. Назовите лица, ответственные только за свои поступки. Они не принимают никаких решений и ни за кем не наблюдают
13. Назовите внешних специалистов или фирмы, нанимаемые предприятием для периодической (довольно редкой) проверки организации и функционирования всей системы безопасности
14. Назовите лицо, которое проводит расчет и перерасчет рисков, ответственен за поиск самой свежей информации об обнаруженных уязвимостях в используемом в фирме программном обеспечении и в целом в стандартных алгоритмах
15. В каком криптоалгоритме единицей кодирования является блок из нескольких байтов?

Вопросы для проверки уровня обученности "владеть":
1. Рассчитайте значение закрытого ключа в криптоалгоритме RSA, если параметры шифрования p=5 и q=7
2. Рассчитайте значение закрытого ключа в криптоалгоритме RSA, если параметры шифрования p=11 и q=13
3. Рассчитайте значение закрытого ключа в криптоалгоритме RSA, если параметры шифрования p=3 и q=7
4. Рассчитайте значение открытого ключа в криптоалгоритме RSA, если параметры шифрования p=5 и q=7, закрытый ключ d=5
5. Зашифруйте криптоалгоритмом RSA букву Б, которой соответствует значение 2, если параметры шифрования p=5 и q=7
6. Расшифруйте криптоалгоритмом RSA зашифрованную букву, значение которой 32, если параметры шифрования p=5 и q=7
7. Напишите фрагмент программы на Pascal, в котором для алгоритма Rijndael происходит ввод 9 символов текста для шифрования.
8. Напишите фрагмент программы на Pascal, в котором для алгоритма Rijndael происходит прибавление к первоначальной матрице единичной матрицы.
9. Напишите фрагмент программы на Pascal, в котором для алгоритма Rijndael происходит заполнение единичной матрицы.
10. Напишите фрагмент программы на Pascal, в котором для расшифровки алгоритмом Rijndael происходит обмен местами первой и последней строки двумерного массива.
11. Напишите фрагмент программы на Pascal, в котором для расшифровки алгоритмом Rijndael происходит обмен местами первого и последнего столбца двумерного массива.
12. Напишите фрагмент программы на Pascal, в котором для расшифровки алгоритмом Rijndael происходит уменьшение всех элементов двумерного массива на 2
13. Напишите фрагмент программы на Pascal, в котором происходит описание файловой переменной
14. Напишите фрагмент программы на Pascal, в котором происходит запись символьного массива из 9 символов в файл
15. Напишите фрагмент программы на Pascal, в котором происходит чтение из файла символов и записи в массив

Итоговое тестирование к зачету
(Компетенция ОПК-4)
1. Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена; нарушение этой категории называется хищением либо раскрытием информации

4. Гарантия того, что при необходимости можно будет доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой; отличие этой категории от предыдущей в том, что при подмене автора, кто-то другой пытается заявить, что он автор сообщения, а при нарушении апеллируемости – сам автор пытается "откреститься" от своих слов, подписанных им однажды.
конфиденциальность
целостность
аутентичность
апеллируемость

5. Гарантия того, что система ведет себя в нормальном и внештатном режимах так, как запланировано
надежность
точность
контроль доступа
контролируемость

6 Уровень модели OSI, который отвечает за доставку больших сообщений по линиям с коммутацией пакетов. Так как в подобных линиях размер пакета представляет собой обычно небольшое число (от 500 байт до 5 килобайт), то для передачи больших объемов информации их необходимо разбивать на передающей стороне и собирать на приемной.
Физический уровень
Канальный уровень
Сетевой уровень
Транспортный уровень
Сеансовый уровень

7. Уровень модели OSI, который отвечает за процедуру установления начала сеанса и подтверждение (квитирование) прихода каждого пакета от отправителя получателю.
Физический уровень
Канальный уровень
Сетевой уровень
Транспортный уровень
Сеансовый уровень

8. Непредусмотренное взаимодействие данных между собой и данных с кодом
Интерференция
Нарушение неявных ограничений
Нет верного ответа

9. Какая утилита позволяет определить настройки компьютера для подключения к локальной сети и к сети Internet
Ipconfig
ping
tracert
Whois
10. При помощи какой утилиты возможно исследование топологии фрагментов сети Internet
Ipconfig
ping
tracert
Whois

11. Для зашифровки и расшифровки сообщения используется один и тот же блок информации (ключ)
Симметричные криптоалгоритмы
Асимметричные криптоалгоритмы
Тайнопись
Нет верного ответа

12. Алгоритм таков, что для зашифровки сообщения используется один ("открытый") ключ, известный всем желающим, а для расшифровки – другой ("закрытый"), существующий только у получателя.
Симметричные криптоалгоритмы
Асимметричные криптоалгоритмы
Тайнопись
Нет верного ответа

13. Отправитель и получатель производят над сообщением преобразования, известные только им двоим
Симметричные криптоалгоритмы
Асимметричные криптоалгоритмы
Тайнопись
Нет верного ответа

14. В зависимости от характера воздействий, производимых над данными, алгоритмы подразделяются на
Перестановочные и подстановочные
Симметричные криптоалгоритмы и асимметричные криптоалгоритмы
Потоковые и блочные

Симметричные криптоалгоритмы и асимметричные криптоалгоритмы
Потоковые криптоалгоритмы
Нет верного ответа

(Компетенция ОПК-14)
1. Какие законы существуют в Российской Федерации в области компьютерного права? (выбрать не менее двух вариантов)
a. О государственной тайне
b. Об авторском и смежных правах
c. О гражданском долге
d. О правовой охране программ для ЭВМ и БД
e. О правовой ответственности
f. Об информации, информатизации и защищенности информации

2. К аспектам информационной безопасности относятся (выбрать не менее двух вариантов)
a. Дискретность
b. Целостность
c. Конфиденциальность
d. Актуальность
e. Доступность

3. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем называется
a. Информационная война
b. Информационное оружие
c. Информационное превосходство

4. Какой орган обеспечивает безопасность учреждений РФ, находящихся за пределами ее территории, и командированных за границу граждан РФ, имеющих по роду своей деятельности допуск к сведениям, составляющим государственную тайну?
a. Федеральная служба безопасности
b. Федеральная служба контрразведки
c. Служба внешней разведки
d. Федеральная служба по техническому контролю и экспортному контролю

5. Усиление правоприменительной деятельности органов исполнительной власти относится
a. к правовым методам обеспечения информационной безопасности
b. к организационно-техническим методам обеспечения информационной безопасности
c. к экономическим методам обеспечения информационной безопасности
d. к политическим методам обеспечения информационной безопасности

6. Какое из перечисленных устройств используется для передачи данных в виде электрических сигналов?
a) Кабель
b) Спутник
c) Оптический кабель

7. Какие существуют основные уровни обеспечения защиты информации? (выбрать не менее двух вариантов)
a. Законодательный
b. Административный
c. Программно-технический
d. Физический
e. Вероятностный
f. Процедурный
g. Распределительный

8. Физические средства защиты информации
a. Средства, которые реализуются в виде автономных устройств и систем
b. Устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу.
c. Это программы, предназначенные для выполнения функций, связанных с защитой информации
d. Средства, которые реализуются в виде электрических, электромеханических и электронных устройств.

9. В чем заключается основная причина потерь информации, связанной с ПК
a. С глобальным хищением информации
b. С появление Интернета
c. С недостаточной образованностью в области безопасности

10. Технические средства защиты информации
a. Средства, которые реализуются в виде автономных устройств и систем
b. Устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой по стандартному интерфейсу

a. Разделение информации на группы так, чтобы нарушение защиты одной группы информации не влияло на безопасность других групп информации
b. Разделение объектов защиты на группы так, чтобы нарушение защиты одной группы не влияло на безопасность других групп

12. Какой документ устанавливает порядок обработки персональных данных в России?
a) Конституция Российской Федерации
b) Федеральный закон "Об информации, информационных технологиях и защите информации"
c) Федеральный закон "О персональных данных"

13. Какой орган в России осуществляет государственный контроль в области защиты информации?
a) ФСБ
b) МВД
c) Роскомнадзор

14. Какой из перечисленных методов шифрования считается самым старым?
a) Шифр Цезаря
b) Шифр Виженера
c) Шифр Энигма

15. Какой из перечисленных алгоритмов шифрования является симметричным?
a) RSA
b) AES
c) DSA

Итоговое тестирование к экзамену
(Компетенция ОПК-4)
1. В зависимости от размера блока информации криптоалгоритмы делятся на:
Перестановочные и подстановочные
Симметричные криптоалгоритмы и асимметричные криптоалгоритмы
Потоковые и блочные
Нет верного ответа

2. Алгоритм сжатия ориентирован на неосмысленные последовательности символов какого-либо алфавита.
Алгоритм Хаффмана
Алгоритм Лемпеля-Зива
Алгоритм Rijndael
Алгоритм TEA

3. Алгоритм сжатия основан наоборот на корреляциях между расположенными рядом символами алфавита (словами, управляющими последовательностями, заголовками файлов фиксированной структуры)
Алгоритм Хаффмана
Алгоритм Лемпеля-Зива
Алгоритм Rijndael
Алгоритм TEA

4. В каком криптоалгоритме единицей кодирования является один бит?
Потоковые шифры
Блочные шифры
Подстановочные криптоалгоритмы
Перестановочные криптоалгоритмы

5. В каком криптоалгоритме единицей кодирования является блок из нескольких байтов?
Потоковые шифры
Блочные шифры
Подстановочные криптоалгоритмы
Перестановочные криптоалгоритмы

6. Лицо, непосредственно работающее с данной информацией. Зачастую только он в состоянии реально оценить класс обрабатываемой информации, а иногда и рассказать о нестандартных методах атак на нее (узкоспецифичных для этого вида данных).
Специалист по информационной безопасности
Владелец информации
Поставщик аппаратного и программного обеспечения
Линейный менеджер

7. Обычно стороннее лицо, которое несет ответственность перед фирмой за поддержание должного уровня информационной безопасности в поставляемых им продуктов.
Специалист по информационной безопасности
Владелец информации
Поставщик аппаратного и программного обеспечения

Владелец информации
Поставщик аппаратного и программного обеспечения
Линейный менеджер

9. Лица, ответственные только за свои поступки. Они не принимают никаких решений и ни за кем не наблюдают
Специалист по информационной безопасности
Владелец информации
Оператор
Линейный менеджер

10. Внешние специалисты или фирмы, нанимаемые предприятием для периодической (довольно редкой) проверки организации и функционирования всей системы безопасности
Специалист по информационной безопасности
Владелец информации
Оператор
Аудиторы

11. Среднее максимальное время отказа для информации 3 класса безотказности
1 день
2 часа
12 минут
20 минут

12. Среднее максимальное время отказа для информации 2 класса безотказности
1 день
2 часа
12 минут
20 минут

13. Среднее максимальное время отказа для информации 1 класса безотказности
1 день
2 часа
12 минут
20 минут

14. Среднее максимальное время отказа для информации 0 класса безотказности
1 день
2 часа
12 минут
20 минут

15. В каком криптоалгоритме единицей кодирования является один бит?
Тайнопись
Перестановочные
Подстановочные
Потоковые

(Компетенция ОПК-14)
1. Какая технология используется для передачи информации по оптоволоконному кабелю?
a. Электричество
b. Свет
c. Звук

2. Какая технология используется для защиты информации в беспроводных сетях?
a. Шифрование
b. Физические барьеры
c. Интерференция

3. Какой алгоритм шифрования является симметричным?
a. RSA
b. AES
c. ElGamal

4. Какая технология используется для защиты информации на физическом уровне в сетях?
a. Фильтрация трафика
b. Шифрование данных
c. Контроль доступа

5. Какой алгоритм шифрования является ассиметричным?
a. Blowfish

b. DES
c. RSA

6. Какой метод используется для оценки сложности алгоритма шифрования?
a. Анализ частотности
b. Анализ времени выполнения
c. Криптоанализ

7. Какая технология используется для защиты информации на уровне приложений?
a. Антивирусное ПО
b. Фаервол
c. Подписывание и проверка цифровых подписей

8. Какой метод используется для проверки подлинности сообщения?
a. Цифровая подпись
b. Шифрование
c. Фильтрация трафика

9. Какая технология используется для защиты информации на уровне операционной системы?
a. Антивирусное ПО
b. Фаервол
c. Пользовательские права доступа

10. Какой метод используется для защиты информации от атак типа "отказ в обслуживании"?
a. Фильтрация трафика
b. Резервное копирование
c. Доступность и отказоустойчивость систем

11. Какие элементы алгебры используются в криптографии?
a) Коммутативность, ассоциативность, дистрибутивность
b) Коммутативность, ассоциативность, идемпотентность
c) Коммутативность, антиассоциативность, дистрибутивность
d) Нет правильного ответа

12. Что такое уязвимость страницы веб-сайта?
a) Способность страницы выдерживать большое количество запросов
b) Способность страницы защищать от атак хакеров
c) Способность страницы обеспечивать конфиденциальность данных
d) Способность страницы быть защищенной от вредоносных программ

13. Какие технические средства используются для защиты информации?
a) Брандмауэры, антивирусы, VPN
b) Принтеры, сканеры, копировальные аппараты
c) Серверы, маршрутизаторы, коммутаторы
d) Нет правильного ответа

14. Какие алгоритмы шифрования относятся к симметричным?
a) RSA
b) AES
c) Diffie-Hellman
d) ECC

15. Какие алгоритмы шифрования относятся к асимметричным?
a) RSA
b) AES
c) Blowfish
d) RC4

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). Эссе должно содержать ссылки на источники. Оригинальность текста должна быть от 80% по программе антиплагиата.

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

Тестирование – это не только форма контроля, но и метод углубления, закрепления знаний обучающихся, так как в ходе собеседования преподаватель разъясняет сложные вопросы, возникающие у обучающегося в процессе изучения учебного материала. Однако тестирование не консультация и не экзамен. Его задача добиться глубокого изучения отобранного материала, пробудить у обучающегося стремление к чтению дополнительной экономической литературы. Зачет завершает изучение определенного раздела учебного курса и должен показать умение обучающегося использовать полученные знания в ходе подготовки и сдачи тестирования при ответах на экзаменационные вопросы. Тестирование может проводиться в устной или письменной форме. Подготовка к тестированию начинается с установочной консультации преподавателя, на которой он разъясняет развернутую тематику проблемы, рекомендует литературу для изучения и объясняет процедуру проведения тестирования. Как правило, на самостоятельную подготовку к тестированию обучающемуся отводится 2-3 недели. Подготовка включает в себя изучение рекомендованной литературы и (по указанию преподавателя) конспектирование важнейших источников. Тестирование проводится в форме индивидуальной беседы преподавателя с каждым обучающимся или беседы в небольших группах (3-5 человек). Обычно преподаватель задает несколько кратких конкретных вопросов, позволяющих выяснить степень добросовестности работы с литературой, контролирует конспект. Далее более подробно обсуждается какая-либо сторона проблемы, что позволяет оценить уровень понимания. Проведение тестирования позволяет обучающемуся приобрести опыт работы над первоисточниками, что в дальнейшем поможет с меньшими затратами времени работать над литературой при подготовке к промежуточной аттестации.

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

В ходе подготовки к зачету студент, в первую очередь, должен систематизировать знания, полученные в ходе изучения дисциплины. К зачету 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 и умений, которыми студент должен владеть;
- тематическими планами лекций, семинарских занятий;
- учебниками, учебными пособиями по дисциплине, а также электронными ресурсами;
- перечнем вопросов к зачету.
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.

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

7.1. Рекомендуемая литература	
7.1.1. Основная литература	
Л.1.1	Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность. Лабораторный практикум + еПриложение [Электронный ресурс]:Учебное пособие. - Москва: КноРус, 2023. - 131 с. – Режим доступа: https://book.ru/book/949452
Л.1.2	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.1.3	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
7.2. Лицензионное и свободно распространяемое программное обеспечение в том числе отечественного производства	
7.2.1	Kaspersky Endpoint Security
7.2.2	Microsoft Office 2013 Standard
7.2.3	Microsoft®WINHOME 10 Russian Academic OLP lLicense NoLevel Legalization GetGenuine
7.2.4	Creative Cloud for Teams Multiple Platforms Multi European Languages Subscription 12 months L2 (10-49) Named EDU
7.3. Перечень профессиональных баз данных, информационных справочных систем и ресурсов сети Интернет	
7.3.1	Электронно-библиотечная система "Лань". Режим доступа: https://e.lanbook.com/
7.3.2	Электронно-библиотечная система "Университетская библиотека онлайн". Режим доступа: https://biblioclub.ru/
7.3.3	Электронно-библиотечная система "BOOK.ru". Режим доступа: https://book.ru/
7.3.4	ПЛАТФОРМА ОНЛАЙН-ОБРАЗОВАНИЯ «РАЗУМ». Режим доступа: https://razoom.mgutm.ru/
7.3.5	Научная электронная библиотека "eLIBRARY.RU". Режим доступа: https://www.elibrary.ru/
7.3.6	Единое окно доступа к образовательным ресурсам. Режим доступа: http://window.edu.ru/
7.3.7	База данных международного индекса научного цитирования Scopus. Режим доступа: http://www.scopus.com/

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1	Адрес: 453850, Республика Башкортостан, р-н Мелеузовский, г. Мелеуз, ул. Смоленская, д. 34, строение 1: аудитория 16-303 - Лаборатория «Интернет технологии» Учебная аудитория для проведения занятий лабораторного и практического типа; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации : Рабочие места обучающихся; Рабочее место преподавателя; Ноутбук; Проектор переносной; Экран переносной; Классная доска; 10 рабочих мест обучающихся оснащенные ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду Университета

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

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры

Информационные технологии и системы управления

Протокол от __ _____ 2025 г. № __
И.о. зав. кафедрой Одинокова Е.В._____

Рабочая программа согласована на заседании выпускающей кафедры

Информационные технологии и системы управления

Протокол от __ _____ 2025 г. № __
И.о. зав. кафедрой Одинокова Е.В. _____

==========

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

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры

Информационные технологии и системы управления

Протокол от __ _____ 2026 г. № __
И.о. зав. кафедрой _____

Рабочая программа согласована на заседании выпускающей кафедры

Информационные технологии и системы управления

Протокол от __ _____ 2026 г. № __
И.о. зав. кафедрой _____

==========

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

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры

Информационные технологии и системы управления

Протокол от __ _____ 2027 г. № __
И.о. зав. кафедрой _____

Рабочая программа согласована на заседании выпускающей кафедры

Информационные технологии и системы управления

Протокол от __ _____ 2027 г. № __
И.о. зав. кафедрой _____

==========

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

Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры

Информационные технологии и системы управления

Протокол от __ _____ 2028 г. № __
И.о. зав. кафедрой _____

Рабочая программа согласована на заседании выпускающей кафедры

Информационные технологии и системы управления

Протокол от __ _____ 2028 г. № __
И.о. зав. кафедрой _____