

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: КУЗНЕЦОВ АЛЕКСАНДР ИГОРЕВИЧ
 Должность: РЕКТОР
 Дата подписания: 06.10.2026 16:04:21
 Уникальный программный ключ:
 0ec0d544ced914f6d2e031d381fc0ed0880d90a0



МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ
ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ЮУрГГПУ»)

РАБОЧАЯ ПРОГРАММА

Шифр	Наименование дисциплины (модуля)
Б1.В.ДВ	Криптографические методы защиты информации

Код направления подготовки	44.03.04
Направление подготовки	Профессиональное обучение (по отраслям)
Наименование (я) ОПОП (направленность / профиль)	Информационные технологии и робототехника
Уровень образования	бакалавр
Форма обучения	заочная

Разработчики:

Должность	Учёная степень, звание	Подпись	ФИО
Доцент	кандидат педагогических наук		Гафарова Елена Аркадьевна

Рабочая программа рассмотрена и одобрена (обновлена) на заседании кафедры (структурного подразделения)

Кафедра	Заведующий кафедрой	Номер протокола	Дата протокола	Подпись
Кафедра автомобильного транспорта, информационных технологий и методики обучения техническим дисциплинам	Руднев Валерий Валентинович	3	18.11.2025	

ОГЛАВЛЕНИЕ

1. Пояснительная записка	3
2. Трудоемкость дисциплины (модуля) и видов занятий по дисциплине (модулю)	4
3. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий	5
4. Учебно-методическое и информационное обеспечение дисциплины	9
5. Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)	10
6. Методические указания для обучающихся по освоению дисциплины	13
7. Перечень образовательных технологий	14
8. Описание материально-технической базы	15

1. ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

1.1 Дисциплина «Криптографические методы защиты информации» относится к модулю части, формируемой участниками образовательных отношений, Блока 1 «Дисциплины/модули» основной профессиональной образовательной программы по направлению подготовки 44.03.04 «Профессиональное обучение (по отраслям)» (уровень образования бакалавр). Дисциплина является дисциплиной по выбору.

1.2 Общая трудоемкость дисциплины составляет 2 з.е., 72 час.

1.3 Изучение дисциплины «Криптографические методы защиты информации» основано на знаниях, умениях и навыках, полученных при изучении обучающимися следующих дисциплин: «Аппаратные средства вычислительной техники», «Информатика», «Компьютерные коммуникации и сети», «Операционные системы и среды».

1.4 Дисциплина «Криптографические методы защиты информации» формирует знания, умения и компетенции, необходимые для освоения следующих дисциплин: «Администрирование информационных систем», «Аппаратно-программное обеспечение ИБ», «Всероссийское чемпионатное движение "Профессионалы"», «Информационное право», «Информационные системы в образовании».

1.5 Цель изучения дисциплины:

освоение студентами основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике

1.6 Задачи дисциплины:

1) дать основы системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов

2) добиться понимания обучающимися принципов разработки шифров

3) ознакомить с математическими методами, используемыми в криптографии

1.7 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы:

№ п/п	Код и наименование компетенции по ФГОС
Код и наименование индикатора достижения компетенции	
1	ПК-6 способен подбирать методы предпроектного анализа для решения поставленной задачи, методы проектирования необходимого отраслевого обеспечения для решения профессиональных задач
	ПК.6.1 Знать методы предпроектного анализа для решения поставленной задачи.
	ПК.6.2 Уметь подбирать методы предпроектного анализа для решения поставленной задачи.
	ПК.6.3 Владеть методами предпроектного анализа для решения поставленной задачи.

№ п/п	Код и наименование индикатора достижения компетенции	Образовательные результаты по дисциплине
1	ПК.6.1 Знать методы предпроектного анализа для решения поставленной задачи.	З.1 Знать методы предпроектного анализа для решения поставленной задачи.
2	ПК.6.2 Уметь подбирать методы предпроектного анализа для решения поставленной задачи.	У.1 Уметь подбирать методы предпроектного анализа для решения поставленной задачи.
3	ПК.6.3 Владеть методами предпроектного анализа для решения поставленной задачи.	В.1 Владеть методами предпроектного анализа для решения поставленной задачи.

2. ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ (МОДУЛЯ) И ВИДОВ ЗАНЯТИЙ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Наименование раздела дисциплины (темы)	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Итого часов
	Л	ЛЗ	СРС	
Итого по дисциплине	2	4	62	68
Первый период контроля				
<i>Основные понятия криптографии</i>	2		20	22
История криптографии. Исторические шифры			10	10
Основные понятия криптографии	2			2
Математическая модель шифра. Теория секретности Шеннона			10	10
<i>Симметричное шифрование</i>		4	10	14
Шифры Цезаря, лозунговый шифр, атбаш		2		2
Шифры перестановки, транспортный, Виженера		2		2
Шифры гаммирования			10	10
<i>Асимметричное шифрование и цифровая подпись</i>			32	32
Основные понятия асимметричного шифрования: методы, принцип, алгоритмы			10	10
Схемы цифровой подписи.			10	10
Криптографические протоколы			12	12
Итого по видам учебной работы	2	4	62	68
<i>Форма промежуточной аттестации</i>				
Зачет				4
Итого за Первый период контроля				72

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ), СТРУКТУРИРОВАННОЕ ПО ТЕМАМ (РАЗДЕЛАМ) С УКАЗАНИЕМ ОТВЕДЕННОГО НА НИХ КОЛИЧЕСТВА АКАДЕМИЧЕСКИХ ЧАСОВ И ВИДОВ УЧЕБНЫХ ЗАНЯТИЙ

3.1 Лекции

Наименование раздела дисциплины (модуля)/ Тема и содержание	Трудоемкость (кол-во часов)
1. Основные понятия криптографии	2
Формируемые компетенции, образовательные результаты: ПК-6: 3.1 (ПК.6.1)	
1.1. Основные понятия криптографии История криптографии. Исторические шифры 2 Основные этапы становления криптографии как науки. Классификация шифров. Шифры замены, перестановки, гаммирования. Композиции шифров. Примеры исторических ручных и машинных шифров. Шифр Цезаря. Шифр простой замены Учебно-методическая литература: 1, 2	2

3.2 Лабораторные

Наименование раздела дисциплины (модуля)/ Тема и содержание	Трудоемкость (кол-во часов)
1. Симметричное шифрование	4
Формируемые компетенции, образовательные результаты: ПК-6: У.1 (ПК.6.2)	
1.1. Шифры Цезаря, лозунговый шифр, атбаш Цель работы: изучение различных методов защиты информации Теоретическая справка Проблемой защиты информации путем ее преобразования занимается криптология (kryptos – тайный, logos – наука). Криптография занимается поиском и исследованием математических методов преобразования информации. Перечислим основные понятия: Алфавит – конечное множество используемых для кодирования информации знаков. Текст – упорядоченный набор из элементов алфавита. Шифрование – преобразовательный процесс Дешифрование – обратный шифрованию процесс. На основе ключа зашифрованный текст преобразуется в исходный. Ключ – информация, необходимая для беспрепятственного шифрования и дешифрования исходных текстов. Существует много различных методов шифрования. Рассмотрим некоторые из них. Методы перестановки. Этот метод заключается в том, что символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов. Рассмотрим некоторые разновидности этого метода. Самая простая перестановка – написать исходный текст задом наперед и одновременно разбить шифрограмму на пятёрки букв. Например из фразы ПУСТЬ БУДЕТ ТАК КАК МЫ ХОТЕЛИ получим сделаем шифротекст: в исходной фразе до кратности пяти не хватает одной буквы. Допишем в конец любую букву и перевернем фразу: ОИЛЕТ ОХЫМК АККАТ ТЕДУБ ЫТСУП. Задание. Зашифруйте полученную у преподавателя фразу всеми методами перестановки. Отчет оформите в текстовом редакторе Microsoft Word. Зашифруйте фразу методом гаммирования. Отчет оформите в программе Microsoft Excel. Расшифруйте полученную у преподавателя информацию. Отчет оформите в программе Microsoft Excel. Учебно-методическая литература: 1, 2, 3	2
1.2. Шифры перестановки, транспортный, Виженера Шифры перестановки, транспортный, Виженера	2

Задание на лабораторную работу. В лабораторной работе необходимо зашифровать свою фамилию с помощью следующих шифров: - шифра Цезаря; - лозунгового шифра; - полибианского квадрата; - шифрующей системы Трисемуса; - шифра Playfair; - системы омофонов (допускается для каждой буквы алфавита привести всего по две шифрозамены, т.е. принять, что все буквы имеют одинаковую вероятность появления в текстах); - шифра Виженера. При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение. Учебно-методическая литература: 1, 2 Профессиональные базы данных и информационные справочные системы: 1	2
--	---

3.3 СРС

Наименование раздела дисциплины (модуля)/ Тема для самостоятельного изучения	Трудоемкость (кол-во часов)
1. Основные понятия криптографии	20
Формируемые компетенции, образовательные результаты: ПК-6: 3.1 (ПК.6.1)	
1.1. История криптографии. Исторические шифры Задание для самостоятельного выполнения студентом: Методика и порядок выполнения работы 1. Изучить теоретический материал работы. 2. Провести исследование системы одноалфавитной замены и алгоритма Студенты делятся на две подгруппы. В первой подгруппе студенты выбирают ключевые слова, а так же получают текст, выданный преподавателем. Затем они строят таблицу и осуществляют шифрование текста. Студенты второй подгруппы, получив от студентов первой подгруппы зашифрованное сообщение и необходимый сдвиг, строят таблицу и осуществляют процесс дешифрования. По окончании расшифрования студенты второй подгруппы приступают к процедуре зашифрования с использованием нового ключевого слова. Студенты первой подгруппы, получив ключевое слово и зашифрованный текст, приступают к его расшифрованию. Содержание отчета и его форма Отчет по лабораторной работе, оформленный письменно в рабочей тетради, должен содержать процесс исследования систем по своему варианту и ответы на контрольные вопросы. Вопросы для защиты работы Вопросы к практическому занятию 1. Дайте определение шифра. Какие виды шифров вы знаете. 2. Дайте определение шифра одноалфавитной замены. 3. Назовите основные достоинства и недостатки шифра одноалфавитной замены 4. Дайте определение шифра. Какие виды шифров вы знаете 5. Дайте определение шифра простой подстановки замены 6. Назовите основные достоинства и недостатки шифра Учебно-методическая литература: 1, 2	10
1.2. Математическая модель шифра. Теория секретности Шеннона Задание для самостоятельного выполнения студентом: Задание для самостоятельного выполнения студентом: Учебный комплексный проект: «Разработка криптографической программы Задание: разработать программу, реализующую процедуры шифрования и расшифрования по стандарту. Программа должна выдавать промежуточные	10

результаты шифрования/расшифрования. Содержание пояснительной записки. Оглавление 1. Краткие сведения о процедуре шифрования 2.1. Общая схема шифрования. 2.2. Исходный текст процедуры шифрования. 2.3. Пример шифрования и расшифрования (исходное сообщение, ключ, ключевые элементы k_i, начальная перестановка, полублоки H_i и L_i, $f(k_i, L_i)$, $H_i f(k_i, L_i)$, конечная перестановка). 3. Руководство пользователя программы. Работа над проектом Учебно-методическая литература: 1, 2 Профессиональные базы данных и информационные справочные системы: 1, 2, 3	10
2. Симметричное шифрование	10
Формируемые компетенции, образовательные результаты: ПК-6: У.1 (ПК.6.2)	
2.1. Шифры гаммирования Задание для самостоятельного выполнения студентом: Задание для самостоятельного выполнения студентом: Учебный комплексный проект: «Разработка криптографической программы Задание: разработать программу, реализующую процедуры шифрования и расшифрования по стандарту. Программа должна выдавать промежуточные результаты шифрования/расшифрования. Содержание пояснительной записки. Оглавление 1. Краткие сведения о процедуре шифрования 2.1. Общая схема шифрования. 2.2. Исходный текст процедуры шифрования. 2.3. Пример шифрования и расшифрования (исходное сообщение, ключ, ключевые элементы k_i, начальная перестановка, полублоки H_i и L_i, $f(k_i, L_i)$, $H_i f(k_i, L_i)$, конечная перестановка). 3. Руководство пользователя программы. Работа над проектом Учебно-методическая литература: 2, 3 Профессиональные базы данных и информационные справочные системы: 1, 3	10
3. Асимметричное шифрование и цифровая подпись	32
Формируемые компетенции, образовательные результаты: ПК-6: В.1 (ПК.6.3)	
3.1. Основные понятия асимметричного шифрования: методы, принцип, алгоритмы Задание для самостоятельного выполнения студентом: Рассмотреть возможные исходы криптоанализа Изучить методы криптоанализа и их влияние на развитие криптографии Оценить предельные возможности по взлому шифров методом полного перебора ключей Проанализировать применимость различных типов криптоатак к симметричным и асимметричным криптосистемам и хеш-функциям Ознакомиться с перспективными технологиями криптоанализа Учебно-методическая литература: 2, 3 Профессиональные базы данных и информационные справочные системы: 2	10
3.2. Схемы цифровой подписи. Задание для самостоятельного выполнения студентом: Составить конспект. Схемы формирования ЭЦП, базирующиеся на шифровании с открытым ключом, принципиально уязвимы. Эффективность используемых на практике схем формирования ЭЦП, основанных на криптографии с открытым ключом, с точки зрения быстродействия, является достаточно низкой. Современные практические реализации схем ЭЦП являются уязвимыми. Учитывая бурное развитие вычислительных мощностей современных компьютерных	10

систем и математических методов криптоанализа, практическая схема цифровой подписи должна гарантировать достаточный уровень защиты на годы вперед. При использовании ЭЦП объектом защиты наряду с самим объектом является и его ЭЦП. Учебно-методическая литература: 1, 2 Профессиональные базы данных и информационные справочные системы: 1	10
3.3. Криптографические протоколы Задание для самостоятельного выполнения студентом: Изучить информационные источники [ISO 7498-2:1989] ISO 7498-2:1989. Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture: Standard / ISO/IEC JTC 1 Information technology. — 02.1989. — URL: www.iso.org/standard/15841.html. [AVISPA] Automated Validation of Internet Security Protocols and Applications (AVISPA): IST-2001-39252. Deliverable 6.1 'List of Selected Problems'. Properties (Goals). — 2003. — URL: www.avispa-project.org/delivs/6.1/d6-1/node3.html [Cheremushkin] Черёмушкин А. В. Криптографические протоколы: основные свойства и уязвимости // Прикладная дискретная математика. — 2009. — нояб. — вып. 2. — с. 115—150. — URL: cyberleninka.ru/article/n/kriptograficheskie-protokoly-osnovnye-svoystva-i-uyazvimosti.pdf - сделать дайджест Учебно-методическая литература: 1, 2 Профессиональные базы данных и информационные справочные системы: 1, 2, 3	12

4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Ссылка на источник в ЭБС
Основная литература		
1	Бутакова Н.Г. Криптографические методы и средства защиты информации [Электронный ресурс]: учебное пособие/ Бутакова Н.Г., Федоров Н.В.— Электрон. текстовые данные.— Санкт-Петербург: Интермедия, 2017.— 384 с	
2	Бескид П.П. Криптографические методы защиты информации. Часть 1. Основы криптографии [Электронный ресурс]: учебное пособие/ Бескид П.П., Тагарникова Т.М.— Электрон. текстовые данные.— Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010.— 95 с.	
Дополнительная литература		
3	Бескид П.П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Электронный ресурс]: учебное пособие/ Бескид П.П., Тагарникова Т.М.— Электрон. текстовые данные.— Санкт-Петербург: Российский государственный гидрометеорологический университет, 2010.— 104 с.	

4.2. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

№ п/п	Наименование базы данных	Ссылка на ресурс
1	Каталог электронных образовательных ресурсов	http://fcior.edu.ru
2	Единая коллекция цифровых образовательных ресурсов	http://school-collection.edu.ru
3	Яндекс–Энциклопедии и словари	http://slovari.yandex.ru

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

5.1. Описание показателей и критериев оценивания компетенций

Код компетенции по ФГОС				
Код образовательного результата дисциплины	Текущий контроль			Промежуточная аттестация
	Кейс-задачи	Отчет по лабораторной работе	Тест	Зачет/Экзамен
ПК-6				
3.1 (ПК.6.1)			+	+
У.1 (ПК.6.2)		+		+
В.1 (ПК.6.3)	+			+

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

5.2.1. Текущий контроль.

Типовые задания к разделу "Основные понятия криптографии ":

1. Тест

Выберите правильный вариант ответа

Криптосистема обладает следующими чертами: предусматривает использование одного и того же закрытого ключа для шифрования и дешифрования данных, характеризуется высокой скоростью работы, но сложностью безопасной передачи самого этого закрытого ключа. Назовите тип криптосистемы.

Асимметричная криптосистема

Симметричная криптосистема

Криптосистема, использующая инфраструктуру открытых ключей (PKI)

Избыточная криптосистема

2. Выберите правильный вариант ответа

Что из указанного не является предметом изучения криптографии?

Шифрование с открытым ключом

Создание алгоритмов надежной электронной подписи

Метод циклического кода CRC

Защита передаваемых данных от несанкционированного изменения

3. Выберите все правильные варианты ответов

Укажите все верные утверждения о шифровании данных.

Любой известный алгоритм шифрования (исключая абсолютно стойкий шифр) можно взломать, перебрав все возможные варианты ключей шифрования

При сопоставимой криптостойкости длина криптостойкого ключа для симметричного алгоритма шифрования меньше, чем для асимметричного алгоритма

Современные алгоритмы шифрования ГОСТ 28147-89 (Россия) и AES (США) являются асимметричными

Асимметричных алгоритмы шифрования работают медленнее по сравнению с симметричными алгоритмами

Для асимметричных алгоритмов шифрования не известно доказательство нижней оценки их стойкости

4. Выберите правильный вариант ответа

RC4 - это ...

Алгоритм потокового шифрования (stream cipher)

Алгоритм блочного шифрования (block cipher)

Алгоритм асимметричного шифрования (public-key encryption)

Алгоритм хэширования (hash algorithm)

Алгоритм создания цифровой подписи (digital signature)

5. Выберите правильный вариант ответа

Для какого алгоритма шифрования типичной является длина ключа 1024 бит?

RC4
AES
3DES
RSA
ГОСТ 28147-89

Количество баллов: 5

Типовые задания к разделу "Симметричное шифрование":

1. Отчет по лабораторной работе

Шифры перестановки, транспортный, Виженера 2

Задание на лабораторную работу.

В лабораторной работе необходимо зашифровать свою фамилию с помощью следующих шифров:

- шифра Цезаря;
- лозунгового шифра;
- полибианского квадрата;
- шифрующей системы Трисемуса;
- шифра Playfair;
- системы омофонов (допускается для каждой буквы алфавита привести всего по две шифрозамены, т.е. принять, что все буквы имеют одинаковую вероятность появления в текстах);
- шифра Виженера.

При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение

Количество баллов: 20

Типовые задания к разделу "Асимметричное шифрование и цифровая подпись":

1. Кейс-задачи

Задача «Как переставить „шкаф“ так, чтобы не нашли». Цель — узнать о науке криптография и стеганография, узнать их различия, понять их актуальность, изучить и научиться использовать шифры перестановки. В кейсе объединены черты обучающего (поиск и анализ информации по физическим и нефизическим способам защиты информации) и практического (решение конкретной задачи с использованием знаний) кейсов.

Количество баллов: 10

5.2.2. Промежуточная аттестация

Промежуточная аттестация проводится в соответствии с Положением о текущем контроле и промежуточной аттестации в ФГБОУ ВО «ЮУрГГПУ».

Первый период контроля

1. Зачет

Вопросы к зачету:

1. Понятия «информационная безопасность» и «защита информации». Основные составляющие информационной безопасности.
2. Объекты защиты. Категории и носители информации
3. Средства защиты информации
4. Криптография. Основные термины и определения
5. Классификация криптографических систем.
6. Шифры замены. Классификация и основные методы шифрования.
7. Шифры перестановки. Классификация и основные методы шифрования.
8. Шифры гаммирования. Классификация и основные методы шифрования
9. Шифры гаммирования. Способы генерации гаммы. Генераторы гамм
10. Схема режима шифрования DES-ECB.
11. Схема режима шифрования DES-CBC
12. Тройной DES. Сферы применения различных режимов DES
13. Схема режима шифрования простой замены ГОСТ 28147-89.
14. Хэш-функции. Основные понятия и разновидности
15. Электронная цифровая подпись. Общие сведения и разновидности ЭЦП.
16. Протоколы контроля целостности. Разновидности и краткая характеристика.
17. Основные сведения о криптоанализе и атаки на криптосистемы.
18. Классическая стеганография
19. Компьютерная стеганография.

20. Секретные кодовые системы

Типовые практические задания:

1. Протокол идентификации/аутентификации на основе шифрования с открытым ключом

5.3. Примерные критерии оценивания ответа студентов на экзамене (зачете):

Отметка	Критерии оценивания
"Отлично"	- дается комплексная оценка предложенной ситуации - демонстрируются глубокие знания теоретического материала и умение их применять - последовательное, правильное выполнение всех заданий - умение обоснованно излагать свои мысли, делать необходимые выводы
"Хорошо"	- дается комплексная оценка предложенной ситуации - демонстрируются глубокие знания теоретического материала и умение их применять - последовательное, правильное выполнение всех заданий - возможны единичные ошибки, исправляемые самим студентом после замечания преподавателя - умение обоснованно излагать свои мысли, делать необходимые выводы
"Удовлетворительно" ("зачтено")	- затруднения с комплексной оценкой предложенной ситуации - неполное теоретическое обоснование, требующее наводящих вопросов преподавателя - выполнение заданий при подсказке преподавателя - затруднения в формулировке выводов
"Неудовлетворительно" ("не зачтено")	- неправильная оценка предложенной ситуации - отсутствие теоретического обоснования выполнения заданий

6. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

1. Лекции

Лекция - одна из основных форм организации учебного процесса, представляющая собой устное, монологическое, систематическое, последовательное изложение преподавателем учебного материала с демонстрацией слайдов и фильмов. Работа обучающихся на лекции включает в себя: составление или слежение за планом чтения лекции, написание конспекта лекции, дополнение конспекта рекомендованной литературой.

Требования к конспекту лекций: краткость, схематичность, последовательная фиксация основных положений, выводов, формулировок, обобщений. В конспекте нужно помечать важные мысли, выделять ключевые слова, термины. Последующая работа над материалом лекции предусматривает проверку терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. В конспекте нужно обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.

2. Лабораторные

Лабораторные занятия проводятся в специально оборудованных лабораториях с применением необходимых средств обучения (лабораторного оборудования, образцов, нормативных и технических документов и т.п.).

При выполнении лабораторных работ проводятся: подготовка оборудования и приборов к работе, изучение методики работы, воспроизведение изучаемого явления, измерение величины, определение соответствующих характеристик и показателей, обработка данных и их анализ, обобщение результатов. В ходе проведения работ используются план работы и таблицы для записей наблюдений.

При выполнении лабораторной работы студент ведет рабочие записи результатов измерений (испытаний), оформляет расчеты, анализирует полученные данные путем установления их соответствия нормам и/или сравнения с известными в литературе данными и/или данными других студентов. Окончательные результаты оформляются в форме заключения.

3. Зачет

Цель зачета – проверка и оценка уровня полученных студентом специальных знаний по учебной дисциплине и соответствующих им умений и навыков, а также умения логически мыслить, аргументировать избранную научную позицию, реагировать на дополнительные вопросы, ориентироваться в массиве информации.

Подготовка к зачету начинается с первого занятия по дисциплине, на котором обучающиеся получают предварительный перечень вопросов к зачёту и список рекомендуемой литературы, их ставят в известность относительно критериев выставления зачёта и специфике текущей и итоговой аттестации. С самого начала желательно планомерно осваивать материал, руководствуясь перечнем вопросов к зачету и списком рекомендуемой литературы, а также путём самостоятельного конспектирования материалов занятий и результатов самостоятельного изучения учебных вопросов.

По результатам сдачи зачета выставляется оценка «зачтено» или «не зачтено».

4. Тест

Тест это система стандартизированных вопросов (заданий), позволяющих автоматизировать процедуру измерения уровня знаний и умений обучающихся. Тесты могут быть аудиторными и внеаудиторными. Преподаватель доводит до сведения студентов информацию о проведении теста, его форме, а также о разделе (теме) дисциплины, выносимой на тестирование.

При самостоятельной подготовке к тестированию студенту необходимо:

- проработать информационный материал по дисциплине. Проконсультироваться с преподавателем по вопросу выбора учебной литературы;
- выяснить все условия тестирования заранее. Необходимо знать, сколько тестов вам будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.
- работая с тестами, внимательно и до конца прочесть вопрос и предлагаемые варианты ответов; выбрать правильные (их может быть несколько); на отдельном листке ответов выписать цифру вопроса и буквы, соответствующие правильным ответам. В случае компьютерного тестирования указать ответ в соответствующем поле (полях);
- в процессе решения желательно применять несколько подходов в решении задания. Это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант.
- решить в первую очередь задания, не вызывающие трудностей, к трудному вопросу вернуться в конце.
- оставить время для проверки ответов, чтобы избежать механических ошибок.

5. Отчет по лабораторной работе

При составлении и оформлении отчета следует придерживаться рекомендаций, представленных в методических указаниях по выполнению лабораторных работ по дисциплине.

6. Кейс-задачи

Кейс – это описание конкретной ситуации, отражающей какую-либо практическую проблему, анализ и поиск решения которой позволяет развивать у обучающихся самостоятельность мышления, способность выслушивать и учитывать альтернативную точку зрения, а также аргументировано отстаивать собственную позицию.

Рекомендации по работе с кейсом:

1. Сначала необходимо прочитать всю имеющуюся информацию, чтобы составить целостное представление о ситуации; не следует сразу анализировать эту информацию, желательно лишь выделить в ней данные, показавшиеся важными.
2. Требуется охарактеризовать ситуацию, определить ее сущность и отметить второстепенные элементы, а также сформулировать основную проблему и проблемы, ей подчиненные. Важно оценить все факты, касающиеся основной проблемы (не все факты, изложенные в ситуации, могут быть прямо связаны с ней), и попытаться установить взаимосвязь между приведенными данными.
3. Следует сформулировать критерий для проверки правильности предложенного решения, попытаться найти альтернативные способы решения, если такие существуют, и определить вариант, наиболее удовлетворяющий выбранному критерию.
4. В заключении необходимо разработать перечень практических мероприятий по реализации предложенного решения.
5. Для презентации решения кейса необходимо визуализировать решение (в виде электронной презентации, изображения на доске и пр.), а также оформить письменный отчет по кейсу.

7. ПЕРЕЧЕНЬ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

1. Развивающее обучение
2. Проблемное обучение
3. Цифровые технологии обучения
4. Кейс-технологии

8. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ

1. компьютерный класс – аудитория для самостоятельной работы
2. компьютерный класс
3. лаборатория
4. учебная аудитория для семинарских, практических занятий
5. Лицензионное программное обеспечение:
 - Операционная система Windows 10/«Альт Образование» 11
 - Microsoft Office Professional Plus/LibreOffice
 - Антивирусное программное обеспечение Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition
 - Справочная правовая система Консультант плюс
 - 7-zip/Менеджер архивов
 - Adobe Acrobat Reader DC/Просмотрщик pdf и djvu-документов
 - Цифровая образовательная платформа "Сферум"
 - Инструментальная среда Ramus Educational
 - Видео редактор Virtual Dub
 - Интернет-браузер
 - Oracle VM VirtualBox - GNU GPL 2
 - DIA - GNU GPL
6. Специализированное оборудование и технические средства обучения: