МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И.
Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
_____ В.Р. Храмшин

04.02.2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

АТТЕСТАЦИЯ АИС

Направление подготовки (специальность)
10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль/специализация) программы
10.05.03 специализация N 8 "Разработка автоматизированных систем в защищенном исполнении"

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Инетитут энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	5
Семестр	9

Магнитогорск
2025 год

Рабочая программа составлена на основе ФГОС ВО - специалитет по специальности 10.05.03 Информационная безопасность автоматизированных систем (приказ Минобрнауки России от 26.11.2020 г. № 1457)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
03.02.2025, протокол № 5

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
04.02.2025 г. протокол № 3

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
доцент кафедры кафедры ИиИБ, канд. техн. наук _____ У.В. Кузьмина

Рецензент:
начальник отдела информационной
безопасности «КУБ» (АО) , _____ М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2028 - 2029 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2029 - 2030 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2030 - 2031 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2031 - 2032 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ И.И. Баранкова

1 Цели освоения дисциплины (модуля)

Целью дисциплины «Аттестация АИС» является формирование профессиональных навыков аттестационных испытаний ОИ, изучение методик проведения аттестации, овладение методами мониторинга и аудита АС и подготовка к деятельности, связанной с аттестацией АИС в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Дисциплина «Аттестация АИС» рассматривает базовые теоретические понятия, средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Аттестация АИС входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Организация ЭВМ и вычислительных систем

Теория информации

Информатика

Языки программирования

Теория вероятностей, математическая статистика

Математический анализ

Основы информационной безопасности

Дискретная математика

Программно-аппаратные средства обеспечения информационной безопасности

Математическое моделирование распределенных систем

Безопасность систем баз данных

Безопасность сетей ЭВМ

Сети и системы передачи информации

Физические основы передачи информации

Защита информации от утечки по техническим каналам

Организационное и правовое обеспечение информационной безопасности

Основы безопасности цифрового общества

Методы и средства криптографической защиты информации

Виртуальные сети

Технология построения защищенных распределенных приложений

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Управление информационной безопасностью

Производственная - научно-исследовательская работа

Производственная - преддипломная практика

Подготовка к сдаче и сдача государственного экзамена

Методы проектирования систем защиты распределенных информационных систем

Обеспечение информационной безопасности критической информационной инфраструктурой

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Моделирование систем защиты информации

Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

Проектная деятельность

Тестирование систем защиты информации автоматизированных систем

Анализ рисков информационной безопасности

Производственная - практика по получению профессиональных умений и опыта профессиональной деятельности

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Аттестация АИС» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-5 Способен проводить аттестацию объектов на соответствие требованиям по защите информации	
ПК-5.1	Проводит аттестационные испытания объектов вычислительной техники на соответствие требованиям по защите информации
ПК-5.2	Оформляет материалы аттестационных испытаний на соответствие требованиям по защите информации
ПК-5.3	Оформляет аттестат соответствия объектов вычислительной техники требованиям по защите информации

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:

– контактная работа – 76,1 акад. часов:

– аудиторная – 72 акад. часов;

– внеаудиторная – 4,1 акад. часов;

– самостоятельная работа – 32,2 акад. часов;

– в форме практической подготовки – 0 акад. час;

– подготовка к экзамену – 35,7 акад. час

Форма аттестации - экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Общие положения проведения аттестационных испытаний								
1.1 Предмет и содержание дисциплины. Методы проверок и испытаний.	9	1			3	Подготовка к практическому занятию; работа с ЭБС и нормативными документами; подготовка к тестированию	Тестирование	ПК-5.1, ПК-5.2, ПК-5.3
1.2 Цели и задачи аттестационных испытаний.		3			0,5	Подготовка к практическому занятию; работа с ЭБС и нормативными документами; подготовка к тестированию;	Тестирование	ПК-5.1, ПК-5.2, ПК-5.3
Итого по разделу		4			3,5			
2. Мероприятия по контролю за состоянием и эффективностью защиты информации на объекте								
2.1 Описание и классификация объектов информатизации.	9	4	2/2И		3	Подготовка к практическому занятию; работа с ЭБС и нормативными документами; подготовка к тестированию;	Тестирование	ПК-5.1, ПК-5.2, ПК-5.3
2.2 Работы, выполняемые в ходе аттестационных испытаний АС.		6	3/3И		5,7	Подготовка к практическому занятию; работа с ЭБС и	Тестирование	ПК-5.1, ПК-5.2, ПК-5.3

						нормативными документами; подготовка к тестированию		
Итого по разделу		10	5/5И		8,7			
3. Методики проведения аттестации								
3.1 Методика проведения аттестации информационной системы по требованиям защиты персональных данных. Подготовка отчетной документации.	9	6	8/8И		8	Подготовка к практическому занятию; работа с ЭБС и нормативными документами, словарями, энциклопедиями); подготовка к контрольной работе	Контрольная работа	ПК-5.1, ПК-5.2, ПК-5.3
3.2 Методика аттестационных испытаний объектов вычислительной техники по требованиям безопасности информации. Подготовка отчетной документации.		6	8/4,85И		10	Подготовка к практическому занятию; работа с ЭБС и нормативными документами; подготовка к контрольной работе	Контрольная работа	ПК-5.1, ПК-5.2, ПК-5.3
Итого по разделу		12	16/12,85И		18			
4. Методика аттестационных испытаний выделенных помещений по требованиям безопасности информации								
4.1 Условия и порядок проведения аттестационных испытаний ВП.	9	4	5		1	Подготовка к практическому занятию; работа с ЭБС и нормативными документами; подготовка к контрольной работе	Контрольная работа	ПК-5.1, ПК-5.2, ПК-5.3
4.2 Объемы испытаний на соответствие требованиям по защите информации для ВП. Подготовка отчетной документации.		6	10		1	Подготовка к практическому занятию; работа с ЭБС и нормативными документами; подготовка к контрольной работе	Контрольная работа	ПК-5.1, ПК-5.2, ПК-5.3
Итого по разделу		10	15		2			
5. Экзамен								
5.1 Подготовка к экзамену	9					Подготовка к зачету; работа с ЭБС и нормативными документами; изучение материалов лекций	Экзамен	ПК-5.1, ПК-5.2, ПК-5.3

Итого по разделу							
Итого за семестр	36	36/17,85И		32,2		экзамен	
Итого по дисциплине	36	36/17,85И		32,2		экзамен	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины используются:

1) Традиционная технология, включающая в себя объяснение преподавателя на лекциях, самостоятельную работу с учебной и справочной литературой по дисциплине, выполнение заданий по методическим указаниям. 2) Раздельно-компетентностная технология, включающая в себя жесткое структурирование содержания учебного материала, сопровождающаяся обязательными блоками домашних заданий, контрольных работ и тестированием по каждой теме содержания курса. 3) Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отношения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды. 4) Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности обучающихся. 5) Игровые технологии – организация образовательного процесса, основанная на реконструкции моделей поведения Формы учебных занятий с использованием предложенных сценарных условий. 6) Технологии проектного обучения – организация образовательного процесса в соответствии с алгоритмом поэтапного решения проблемной задачи или выполнения учебного задания. Проект предполагает совместную учебно-познавательную деятельность группы обучающихся, направленную на выработку концепции, установление целей и задач, формулировку ожидаемых результатов, определение принципов и методик решения поставленных задач, планирование хода работы, поиск доступных и оптимальных ресурсов, поэтапную реализацию плана работы, презентацию результатов работы, их осмысление и рефлексию. 7) Информационно-коммуникационные образовательные технологии – организация образовательного процесса, основанная на применении специализированных программных сред и технических средств работы с информацией.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины

а) Основная литература:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277 (дата обращения: 19.02.2025).

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL:

https://urait.ru/bcode/493262 (дата обращения: 19.02.2025).

3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491249 (дата обращения: 19.02.2025).

б) Дополнительная литература:

1. Брюхомицкий, Ю.А. Искусственные иммунные системы в информационной безопасности: учебное пособие / Ю. А. Брюхомицкий; Южный федеральный университет. - Ростов-на-Дону; Таганрог: Издательство Южного федерального университета, 2019. - 147 с. - ISBN 978-5-9275-3212-4. - Текст: электронный. - URL: https://new.znanium.com/catalog/product/1088177 (дата обращения: 26.02.2025)

2. Веселов, Г.Е. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог: Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5. - Текст: электронный. - URL: https://new.znanium.com/catalog/product/997108 (дата обращения: 26.02.2025)

5. Сетевая защита информации. Лабораторный практикум : учебное пособие [для вузов] / Д. Н. Мазнин, И. И. Баранкова, У. В. Михайлова, М. В. Афанасьева ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://host.megaprolib.net/MP0109/Download/MObject/2400. - ISBN 978-5-9967-1605-0. - Текст : электронный. (дата обращения: 26.02.2025)

в) Методические указания:

1. Методические указания по выполнению лабораторных работ (Приложение 1)

2. Методические указания по выполнению внеаудиторных самостоятельных работ

(Приложение 2)

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
7Zip	свободно распространяемое ПО	бессрочно
Adobe Audition CS 5.5 Academic Edition	К-615-11 от 12.12.2011	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
eTokenSecurLogon for Oracle	К-271-12 от 16.10.2012	бессрочно
СЗИ Страж NT в.3	К-271-12 от 16.10.2012	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно распространяемое ПО	бессрочно

СКЗИ КриптоПро CSP	К-271-12 от 16.10.2012	бессрочно
VIP Net Client	Д-946-14 от 22.07.2014	бессрочно
VIP Net CryptoService	Д-946-14 от 22.07.2014	бессрочно
Calculate Linux Desktop Xfce	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации ФСТЭК России	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi?ysclid=lujknksfy724757053
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/?ysclid=lujkqy7cnw630508962

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Материально-техническое обеспечение дисциплины включает:

Лекционные аудитории:

- Мультимедийные средства хранения, передачи и представления информации.

Лаборатория технической защиты информации:

1. АКС-1301 Анализатор спектра
2. Комплекс радиомониторинга "Касандра К6" с диапазоном рабочих частот 0,009-6000Мгц
3. Комплекс радиомониторинга "Касандра К21" с диапазоном рабочих частот 0,009-21000Мгц
4. Генератор шума стационарный "ГШ-1000-М"
5. Система виброакустической и акустической защиты "Соната-АВ"
6. Устройство защиты телефонных переговоров от прослушивания и записи "Прокруст-200"
7. Портативный поисковый комплекс амплитудной пеленгации «Касандра С6»
8. Система оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН) Сигурд

Компьютерные классы:

- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

Помещения для самостоятельной работы обучающихся:

- Персональные компьютеры с ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

ПРИЛОЖЕНИЕ 1

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

По дисциплине «Аттестация АИС» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает решение контрольных задач на практических занятиях.

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде решения задач и выполнения упражнений, которые определяет преподаватель для обучающегося

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Примерные задания и вопросы по темам:

Перечень вопросов аудиторных контрольных работ по темам разделов 1-5:

1. Методики проведения аттестации ИС по требованиям защиты ПДн.
2. Цели и задачи аттестационных испытаний.
3. Описание технологического процесса обработки и хранения конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации средств ВТ.
4. Порядок проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ.
5. Условия и порядок проведения аттестационных испытаний объекта ВТ.
6. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ СВТ.
7. Объем испытаний на соответствие требованиям по ЗИ от НСД.
8. Проверка ВП на соответствие организационно-техническим требованиям по защите информации.
9. Условия и порядок проведения аттестационных испытаний ВП.
10. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП.
11. Объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП.
12. Порядок подготовки отчетной документации по аттестации выделенных помещений и средств вычислительной техники, оценка результатов испытаний.
13. Обнаружение атак.
14. Захват сетевого трафика (механизмы захвата сетевого трафика, реализованные в специальном программно-аппаратном обеспечении, например, в Cisco Catalyst 6000 IDS Module или Cisco Secure Integrated Software),
15. Фильтрация с помощью свободно распространяемых утилит,
16. Распознавание атак (сигнатуры первого типа) с использованием утилит и библиотек.
18. Подсистемы СОВ.
19. Обнаружение аномалий в защищаемой системе.
20. Обнаружение злоупотреблений в защищаемой системе.
21. Накопление наиболее характерной статистической информации для каждого параметра оценки.
22. Обучение нейронных сетей значениями параметров оценки.
23. Статистика Байеса.
24. Использование условной вероятности.
25. Экспертные системы.
26. Методы, основанные на моделировании поведения злоумышленника.

ПРИЛОЖЕНИЕ 2

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Компетенция/ Индикатор достижения компетенции	Оценочные средства
ПК-5 Способен проводить аттестацию объектов на соответствие требованиям по защите информации	
ПК-5.1 Проводит аттестационные испытания объектов вычислительной техники на соответствие требованиям по защите информации	1. Методики проведения аттестации ИС по требованиям защиты ПДн. 2. Цели и задачи аттестационных испытаний. 3. Описание технологического процесса обработки и хранения конфиденциальной информации, анализ информационных потоков, определение состава использованных для обработки защищаемой информации средств ВТ. 4. Порядок проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ. 5. Условия и порядок проведения аттестационных испытаний объекта ВТ. 6. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ СВТ.
ПК-5.2 Оформляет материалы аттестационных испытаний на соответствие требованиям по защите информации	1. Произвести измерения ПЭМИН от технических средств и составить протокол аттестационных испытаний 2. Произвести анализ информационных потоков, 3. Произвести проверку механизма обеспечения целостности. 4. Произвести проверку механизма регистрации и учета. 5. Объем испытаний на соответствие требованиям по защите информации от утечки по акустическому и виброакустическому каналам для ВП. 6. Проверка выполнения требований по защите информации от утечки за счет ПЭМИ ОТСС для ВП. 7. Выполнить описание технологического процесса обработки и хранения конфиденциальной информации 8. Произвести анализ информационных потоков 9. Определить состав использованных для обработки защищаемой информации средств ВТ. 10. Составить план проверки на соответствие организационно-техническим требованиям по защите информации объекта ВТ. 11. Определить условия и порядок проведения аттестационных испытаний объекта ВТ. 12. Произвести проверку выполнения требований по защите информации от утечки за счет ПЭМИ СВТ.
ПК-5.3 Оформляет аттестат соответствия объектов	1. Определить объем испытаний на соответствие требованиям по ЗИ от НСД. 2. Произвести аттестационные испытания и составить протокол для объекта информатизации (ОИ) на соответствие требованиям безопасности

Компетенция/ Индикатор достижения компетенции	Оценочные средства
вычислительной техники требованиям по защите информации	информации по направлению «Защита информации от НСД». 3. Разработать методику проведения аттестационных испытаний ОИ в соответствии с моделью угроз. 4. Составить заключение по результатам аттестационных испытаний. 5. Проверка ВП на соответствие организационно-техническим требованиям по защите информации. 6. Условия и порядок проведения аттестационных испытаний ВП. 7. Порядок подготовки отчетной документации по аттестации выделенных помещений и средств вычислительной техники, оценка результатов испытаний.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме экзамена.

Показатели и критерии оценивания экзамена:

– на оценку **«отлично»** – обучающийся должен показать высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку **«хорошо»** – обучающийся должен показать средний уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач;

– на оценку **«удовлетворительно»** – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации, навыки решения типовых задач;

– на оценку **«неудовлетворительно»** – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки решения типовых задач.

ПРИЛОЖЕНИЕ 3

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Рекомендации направлены на оказание методической помощи студентам при выполнении лабораторных занятий.

Лабораторное занятие – это занятие, проводимое под руководством преподавателя в учебной аудитории (компьютерном классе университета или учебной специализированной лаборатории университета), направленное на углубление научно-теоретических знаний и получение лабораторных навыков решения типовых и прикладных задач.

Целью лабораторных занятий является формирование и отработка лабораторных умений и навыков, необходимых в последующей деятельности обучающихся.

Основными задачами лабораторных занятий являются:

- углубление уровня освоения общекультурных и профессиональных компетенций;
- обобщение, систематизация, углубление, закрепление полученных лабораторных знаний по конкретным темам дисциплин различных циклов;
- приобретение студентами умений и навыков использования современных теоретических знаний в решении конкретных прикладных задач;
- развитие профессионального мышления, профессиональной и познавательной мотивации.

Перечень тем лабораторных работ определяется рабочей программой дисциплины. План лабораторных занятий отвечает общей направленности лекционного курса и соотнесен с ним в последовательности тем.

Структура лабораторного занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущей лабораторной работы, ставится ее цели и задачи, проводиться инструктаж по технике безопасности выполнения работы, проверяется исходный уровень готовности студентов к лабораторной работе (выполнение тестов, контрольные вопросы и т.п.), выдается порядок и условия выполнения лабораторной работы.

На лабораторном занятии преподаватель может использовать разнообразные образовательные технологии (методы IT, работа в команде, case-study, проблемное обучение, учебные дискуссии и т.п.) по своему выбору для достижения качественного уровня обучения.

Правила по технике безопасности для обучающихся при проведении лабораторных работ

Общие правила:

1. Лабораторные работы проводятся под наблюдением преподавателя. К выполнению лабораторных работ студенты допускаются только после прослушивания инструктажа по технике безопасности, правилам поведения, противопожарным мерам в компьютерном классе и специализированных лабораториях.

2. Обучаемый должен строго выполнять правила техники безопасности и санитарно-гигиенические нормы при работе в компьютерных классах и специализированных лабораториях университета.

Порядок выполнения лабораторных работ

При подготовке к выполнению лабораторных работ студент должен повторить теоретический материал, необходимый для выполнения заданий по текущей теме.

Лабораторная работа выполняется каждым студентом самостоятельно, согласно индивидуальному заданию.

Студенты, пропустившие занятия, выполняют лабораторные работы во внеурочное время.

После выполнения каждой лабораторной работы студент демонстрирует результат выполнения преподавателю в виде отчета по лабораторной работе и отвечает на вопросы. Преподаватель оценивает работу в соответствии с заданными критериями оценки лабораторных работ.

Правила оформления результатов и оценивания лабораторной работы

Результаты выполненной лабораторной работы оформляются в соответствии с требованиями к выполнению конкретной работы.

Практическая работа считается выполненной, если студент набрал балл, который составляет

половину максимального количества баллов.

Для оценивания работы прилагаются следующие критерии.

Оценка «отлично» – работа выполнена в полном объеме и без замечаний.

Оценка «хорошо» – работа выполнена правильно с учетом 2-3 несущественных ошибок, исправленных самостоятельно по требованию преподавателя.

Оценка «удовлетворительно» – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

Оценка «неудовлетворительно» – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя, или работа не выполнена.