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

03.02.2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ПЕНТЕСТИНГ

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	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	5
Семестр	10

Магнитогорск
2026 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
22.01.2026, протокол № 5

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
03.02.2026 г. протокол № 5

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 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

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2032 - 2033 учебном году на заседании кафедры Информатики и информационной безопасности

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

1 Цели освоения дисциплины (модуля)

Целями освоения дисциплины «Пентестинг» (тестирование на проникновение) заключаются в формировании у обучающихся знаний, навыков и компетенций, необходимых для выявления и устранения уязвимостей в информационных и автоматизированных системах; составления методик тестирования на проникновение в информационных и автоматизированных системах; подбора инструментальных средств тестирования информационных и автоматизированных систем; составление протоколов тестирования и овладение обучающимися необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВО для специальности 10.05.03 Информационная безопасность автоматизированных систем.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Пентестинг 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

Сети и системы передачи информации

Программно-аппаратные средства обеспечения информационной безопасности

Безопасность систем баз данных

Безопасность сетей ЭВМ

Разработка систем защиты информации автоматизированных систем

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

Обеспечение информационной безопасности критической информационной инфраструктурой

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Форензика

Производственная - научно-исследовательская работа

Производственная - преддипломная практика

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

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

Код индикатора	Индикатор достижения компетенции
ПК-6 Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	
ПК-6.1	Проводит анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем
ПК-6.2	Выявляет уязвимости информационно-технологических ресурсов автоматизированных систем
ПК-6.3	Выявляет основные угрозы безопасности информации в автоматизированных системах
ПК-6.4	Составляет протоколы тестирования систем защиты информации автоматизированных систем

4. Структура, объём и содержание дисциплины (модуля)

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

– контактная работа – 103,8 акад. часов:

– аудиторная – 102 акад. часов;

– внеаудиторная – 1,8 акад. часов;

– самостоятельная работа – 40,2 акад. часов;

– в форме практической подготовки – 0 акад. час;

Форма аттестации - зачет

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. Этичный хакинг								
1.1 Понятие пентеста. Виды пентеста.	10	4	4/4И		6	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к АКР, тестированию, зачету.	тестирование, АКР, защита работ	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4
1.2 Программы Bug Bounty. Принципы и платформы для взаимодействия хакеров и компаний.		6	5/5И		4	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к АКР, тестированию, зачету.	тестирование, АКР, защита работ	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4
1.3 Инструментарий для пентестинга.		6	20/14,8И		6	поиск дополнительной	Рубежный контроль: устная	ПК-6.1, ПК-6.2, ПК-6.3,

						информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к АКР, тестированию, зачету.	защита отчета по выполненным работам по разделу	ПК-6.4
Итого по разделу		16	29/23,8 И		16			
2. Тестирование на проникновение (пентестинг)								
2.1 Активный анализ системы на наличие уязвимостей.	10	4	13		6	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к АКР, тестированию, зачету.	тестирование, АКР, защита работ	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4
2.2 Анализа сетевого трафика для выявления возможных утечек данных.		6	12		8	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями); подготовка к АКР, тестированию, зачету.	тестирование, АКР, защита работ	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4
2.3 Статический анализ кода для выявления потенциальных ошибок, уязвимостей и нарушений правил кодирования.		8	14		10,2	поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиям	Рубежный контроль: устная защита отчета по выполненным работам по разделу	ПК-6.1, ПК-6.2, ПК-6.3, ПК-6.4

						и); подготовка к АКР, тестированию, зачету.		
Итого по разделу		18	39		24,2			
Итого за семестр		34	68/23,8 И		40,2		зачёт	
Итого по дисциплине		34	68/23,8 И		40,2		зачет	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Пентестинг» используются традиционная и модульно-компетентностная технологии.

Реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.

При проведении учебных занятий преподаватель обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств посредством проведения интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализа ситуаций, учета особенностей профессиональной деятельности выпускников и потребностей работодателей.

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, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772(дата обращения: 31.01.2026).

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/441287 (дата обращения: 31.01.2026).

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, 2019. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/437163 (дата обращения: 31.01.2026).

б) Дополнительная литература:

1. Внуков, А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/414083 (дата обращения: 31.01.2026).

2. Зашита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1018901 (дата обращения: 31.01.2026)

3. Брюхомицкий, Ю. А. Искусственные иммунные системы в информационно

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: 31.01.2026)

4. 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: 31.01.2026).

4. Развертывание и настройка виртуальных сетей : учебное пособие [для вузов] / [сост.: В. В. Баранков, И. И. Баранкова, У. В. Михайлова, О. Б. Калугина] ; МГТУ. - Магнитогорск : МГТУ, 2019. - 1 электрон. опт. диск (CD-ROM). - URL: https://host.megaprolib.net/MP0109/Download/MObject/2388. - ISBN 978-5-9967-1305-9. - Текст : электронный (дата обращения: 31.01.2026).

5. Архитектура и принципы работы вычислительных систем : учебное пособие [для вузов] / В. В. Баранков, И. И. Баранкова, М. В. Коновалов, 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/2495. - ISBN 978-5-9967-1306-6. - Текст : электронный (дата обращения: 31.01.2026).

6. Мазнин Д. Н. Администрирование компьютерных сетей : учебное пособие [для вузов] / Д. Н. Мазнин, Ю. А. Мазнина. - Магнитогорск : МГТУ им. Г. И. Носова, 2023. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://host.megaprolib.net/MP0109/Download/MObject/21027. - ISBN 978-5-9967-2906-7. - Текст : электронный (дата обращения: 31.01.2026).

в) Методические указания:

Методические указания по выполнению внеаудиторных самостоятельных работ по дисциплине «Пентестинг» (Приложение 3).

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно

7Zip	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации ФСТЭК России Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-tzi?ysclid=lujknksfy724757053 https://bdu.fstec.ru/?ysclid=lujkqy7cnw630508962
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	https://host.megaprolib.net/MP0109/Web
Электронная база периодических изданий ООО «ИВИС»	https://eivis.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Лекционная аудитория (ауд. 2124, ауд. 226, ауд. 365, ауд. 388 и т.д.)- Мультимедийные средства хранения, передачи и представления информации

Киберполигон «MagTech Cyberlab», ауд. 2113

Компьютерный класс (ауд. 372, ауд. 245, ауд. 247, ауд. 144, ауд. 142 и т.д.) - Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

Аудитория для самостоятельной работы читальные залы библиотеки, ауд 132а - Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

ПРИЛОЖЕНИЕ 1

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

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

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 вопросов по темам:

Перечень контрольных вопросов:

1. Законодательно-правовые основы пентеста
2. Функциональные требования безопасности
3. Требования доверия к безопасности
4. Методологии пентеста
5. Этапы тестирования на проникновение
6. Международные стандарты (OSSTMM, PTES, NIST SP 800-115)
7. Классификации уязвимостей (CVE, CVSS)
8. Принципы этичного хакинга (White Hat Hacking)
9. Знания, необходимые для сдачи экзаменов CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional) и др.
10. Методы взлома и защиты (SQL-инъекции, XSS, CSRF, эксплуатация ОС и сетевых сервисов).
11. Как использовать MITRE ATT&CK в пентесте?
12. Инструменты для работы с MITRE ATT&CK

Пример лабораторной работы.

Анализ и обход механизмов обнаружения угроз в системах класса AV/ID.

1. Выбор и настройка средства защиты.

- Антивирусное ПО
- Система обнаружения вторжений

Установить, настроить и обеспечить работоспособность выбранного СЗИ в изолированной ВМ.
Обеспечить МАКСИМАЛЬНУЮ защиту ВМ, чтобы не допустить распространение ВПО.
Работать только в изолированных средах!
! ВЫПОЛНЯТЬ ЛАБОРАТОРНУЮ ТОЛЬКО НА СВОИХ НОУТБУКАХ/КОМПЬЮТЕРАХ/ВМ !
! ЗАПРЕЩЕНО ИСПОЛЬЗОВАТЬ ИНФРАСТРУКТУРУ ВУЗА ДЛЯ ПРОВЕДЕНИЯ ЛЮБЫХ ЭТАПОВ РАБОТЫ !
! НЕДОПУСТИТЬ РАСПРОСТРАНЕНИЕ ВПО ! ОТВЕТСВЕННОСТЬ НА ВАС !
Как настроить виртуальную среду смотри: тут и тут.

2. Демонстрация обнаружения.

- Для AV:
  - Использовать стандартный тестовый файл **EICAR**.
  - Найти, записать в таблице и сообщить преподавателю о выбранном ВПО с открытым кодом. Проверить ВПО в
    - VT, AnyRun или ином сервисе;

        - На своем подготовленном стенде с установленным СЗИ.;
- Для IDS**:**
    - Найти, записать в таблице и сообщить преподавателю о выбранной сетевой атаке.
    - Найти правила на обнаружение выбранной атаки и провести УСПЕШНУЮ атаку и УСПЕШНОЕ обнаружение, для проверки работоспособности IDS.

Подготовить аналитический отчет об атаке и сигнатурах на основе своего анализа и открытых источников (разборов).

3. Модификация и демонстрация необнаружения.

- Для AV:
    - Модифицируйте открытый код, для обхода ВСЕХ возможных методов (сигнатурный, эвристический, поведенческий, песочницу, в том числе с использованием ML) анализа ВПО;
    - Использовать: обфускацию, упаковку, криптеры, инъекцию кода, fileless подходы, living off the land, полиморфизм и мимикрию, стеганографию.
    - Проведите УСПЕШНУЮ атаку и останьтесь необнаруженным.
- Для IDS:
    - Максимально модифицировать атакуемый трафик, чтобы сигнатура IDS НЕ СРАБОТАЛА, но атака БЫЛА УСПЕШНА.
    - Обязательно использовать НЕСКОЛЬКО различных правил обнаружения атаки (проанализировать в чем их разница?)

4. Аналитическая часть

1. Подготовить отчет о проделанной работе;
2. Максимально передать контекст и суть выбранной атаки;
3. Какие методы применялись для обхода?
4. Какие подходы СЗИ успешно/неуспешно обнаружили атаку?
5. Предложите методы/подходы и их реализацию для обнаружения подобных атак.
6. Для сетевых атак написать правило обнаружения.

ПРИЛОЖЕНИЕ 2

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

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

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ПК-6 Способен проводить анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем		
ПК-6.1	– Проводит анализ структурных и функциональных схем защищенных автоматизированных информационных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем	Вопросы к зачету 1. Законодательно-правовые основы пентеста 2. Функциональные требования безопасности 3. Требования доверия к безопасности 4. Методологии пентеста 5. Этапы тестирования на проникновение 6. Международные стандарты (OSSTMM, PTES, NIST SP 800-115) 7. Классификации уязвимостей (CVE, CVSS) 8. Принципы этичного хакинга (White Hat Hacking) 9. Знания, необходимые для сдачи экзаменов CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional) и др. 10. Методы взлома и защиты (SQL-инъекции, XSS, CSRF, эксплуатация ОС и сетевых сервисов). 11. Как использовать MITRE ATT&CK в пентесте? 12. Инструменты для работы с MITRE ATT&CK
ПК-6.2	Выявляет уязвимости информационно-технологических ресурсов автоматизированных систем	Задания: 1. Провести тестирование механизмов фильтрации данных и трансляции адресов 2. Провести тестирование механизмов идентификации и аутентификации администраторов 3. Провести тестирование механизмов контроля целостности 4. Провести тестирование антивирусной защиты 5. Применение инструментов для пентестинга (Kali Linux, Metasploit, Burp Suite, Nmap, Wireshark и др.).
ПК-6.3	Выявляет основные угрозы безопасности информации в автоматизированных системах	Задания 1. Провести тестировании на проникновение на киберполигоне «MagTech Cyberlab» 2. Провести моделирование действий киберпреступников 3. Провести аудит безопасности сетей, систем, приложений, физической безопасности. 4. Провести аудит безопасности веб-приложения и API. 5. Провести анализ и обход механизмов обнаружения угроз в системах класса AV/IDS.

ПК-6.4	Составляет протоколы тестирования систем защиты информации автоматизированных систем	Вопросы к зачету 1. Структура протокола пентеста 2. Стандарты пентеста (PTES, OWASP, NIST). Задания 1. Составить план и пояснить этапы тестирования дискреционного принципа контроля доступа 2. Составить план и пояснить этапы тестирования мандатного принципа контроля доступа 3. Составить план и пояснить этапы тестирования механизмов очистки памяти 4. Составить план и пояснить этапы тестирования механизмов изоляции модулей 5. Составить план и пояснить этапы тестирования механизмов идентификации и аутентификации субъектов доступа 6. Составить план и пояснить этапы тестирования механизмов контроля целостности 7. Составить план и пояснить этапы тестирования испытаний межсетевых экранов 8. Составить отчет о тестировании на проникновение

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

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

Показатели и критерии оценивания зачета:

– на оценку **«зачтено»** – обучающийся должен успешно пройти запланированные рубежные контроли и показать пороговый уровень знаний на уровне воспроизведения и объяснения информации;

– на оценку **«не зачтено»** – обучающийся не прошел запланированные рубежные контроли и 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 обучающимся при выполнении лабораторных работ.

Лабораторная работа – 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 практических навыков решения типовых и прикладных задач.

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

Основными задачами лабораторных работ являются:

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

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

Структура занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущего занятия, ставится его цели и задачи, проверяется исходный уровень готовности обучающихся к занятию (выполнение тестов, контрольные вопросы и т.п.)

На 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 практических работ

Общие правила:

1. Лабораторные работы проводятся под наблюдением преподавателя. К выполнению лабораторных работ обучающиеся 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 практических работ

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

После выполнения каждой лабораторной работы обучающийся демонстрирует результат выполнения преподавателю, отвечает на вопросы. Преподаватель оценивает работу в соответствии с заданными критериями оценки практических работ.

Правила оформления результатов и оценивания практической работы

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

Работа считается выполненной, если обучающийся набрал балл, который составляет половину максимального количества баллов.

Для оценивания работы прилагается 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 обучающийся не может исправить даже по требованию преподавателя, или работа не выполнена.

ПРИЛОЖЕНИЕ 4

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ВНЕАУДИТОРНЫХ САМОСТОЯТЕЛЬНЫХ РАБОТ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы обучающихся и оказания помощи в самостоятельном изучении теоретического и реализации компетенций обучаемых.

Данные методические указания не являются учебным пособием, поэтому перед началом выполнения самостоятельного задания следует изучить соответствующие разделы лекционных занятий, материалов образовательного портала, разделов основной и дополнительной литературы, представленных в пункте 8. «Учебно-методическое и информационное обеспечение дисциплины (модуля)» данной РПД.

Цели и задачи самостоятельной работы

Цель самостоятельной работы – содействие оптимальному усвоению учебного материала обучающимися, развитие их познавательной активности, готовности и потребности в самообразовании.

Задачи самостоятельной работы:

- повышение исходного уровня владения информационными технологиями;
- углубление и систематизация знаний;
- постановка и решение стандартных задач профессиональной деятельности;
- развитие работы с различной по объему и виду информацией, учебной и научной литературой;
- практическое применение знаний, умений;
- самостоятельно использование стандартных программных средств сбора, обработки, хранения и защиты информации
- развитие навыков организации самостоятельного учебного труда и контроля за его эффективностью.

Виды внеаудиторной самостоятельной работы и формы контроля и время на выполнение каждого вида самостоятельной работы указаны в пункте 4. «Структура и содержание дисциплины» данной РПД.

Порядок выполнения

При выполнении текущей внеаудиторной самостоятельной работы обучающемуся следует придерживаться следующего порядка действий:

1) внимательно изучить соответствующие теоретические разделы дисциплины, пользуясь материалами (лекционными, презентационными, аудио-визуальными):
   a) предоставляемыми преподавателем на лекционных занятиях;
   b) предоставляемыми преподавателем в рамках электронных образовательных курсов;
   c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.
2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.
3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.
4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы с обучающимися группы, в рамках командно-проектной работы, и с преподавателем, в рамках консультационной помощи, реализованной либо в контактной форме, либо средствами информационно-образовательной среды ВУЗа.

Критерии оценки внеаудиторных самостоятельных работ

Качество выполнения внеаудиторной самостоятельной работы обучающихся оценивается посредством текущего контроля самостоятельной работы обучающихся с использованием балльно-рейтинговой системы.

В качестве форм текущего контроля по дисциплине используются: индивидуальные задания, аудиторные контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

- выполняет индивидуальные задания в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.