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

10.02.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

АНАЛИЗ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

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	4
Семестр	7

Магнитогорск
2023 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
09.02.2023, протокол № 5

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
10.02.2023 г. протокол № 7

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
Ст. преподаватель кафедры ИиИБ, канд. техн. наук _____ М.В. Коновалов

Рецензент:
Проректор по цифровизации, канд. техн. наук _____ К.А. Рубан

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 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 2025 - 2026 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 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

1 Цели освоения дисциплины (модуля)

Общей целью дисциплины «Анализ безопасности информационных технологий» является повышение исходного уровня владения информационными технологиями, достигнутого на предыдущей ступени образования, и овладение обучающимися необходимым и достаточным уровнем профессиональных компетенций в соответствии с требованиями ФГОС ВО по специальности «Информационная безопасность автоматизированных систем». Специальными целями дисциплины «Анализ безопасности информационных технологий» являются: изучить функции, методы и алгоритмы и готовые аппаратно-программные решения анализа безопасности информационных технологий; научится применять в промышленности и сетевых средах системы управления событиями информационной безопасности автоматизированных систем; выполнять аудит информационной безопасности информационных систем.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Анализ безопасности информационных технологий входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

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

Информатика

Организация ЭВМ и вычислительных систем

Виртуальные сети

Моделирование угроз информационной безопасности

Сети и системы передачи информации

Безопасность сетей ЭВМ

Безопасность систем баз данных

Организационное и правовое обеспечение информационной безопасности

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

Подготовка к сдаче и сдача государственного экзамена

Производственная - преддипломная практика

Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

Производственная - научно-исследовательская работа

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

В результате освоения дисциплины (модуля) «Анализ безопасности информационных технологий» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей	
ПК-2.1	Разрабатывает профили защиты компьютерных систем
ПК-2.2	Формирует политики безопасности компьютерных систем и сетей
ПК-4 Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей	
ПК-4.1	Применяет инструментальные средства проведения мониторинга защищенности компьютерных систем
ПК-4.2	Применяет методы анализа защищенности компьютерных систем и

	сетей

4. Структура, объём и содержание дисциплины (модуля)

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

– контактная работа – 69,8 акад. часов:

– аудиторная – 68 акад. часов;

– внеаудиторная – 1,8 акад. часов;

– самостоятельная работа – 74,2 акад. часов;

– в форме практической подготовки – 0 акад. час;

Форма аттестации - зачет с оценкой

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. Среда для проведения анализа информационных технологий								
1.1 Технические требования. Физическая и виртуальная испытательные лаборатории. Тестовые ИТ.	7	2,5		3	6	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	семинарское занятие	ПК-2.1, ПК-2.2, ПК-4.1, ПК-4.2
1.2 Параметрирование уязвимых виртуальных сервисов. Metaspoiltable2 и Metaspoiltable 3		3		3	6	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	семинарское занятие	ПК-2.1, ПК-2.2, ПК-4.1, ПК-4.2
Итого по разделу		5,5		6	12			
2. Методология анализа безопасности информационных технологий								

2.1 Стандарты проведения тестирования безопасности ИТ. Методика OWASP.	7	3		3	6	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	семинарское занятие	ПК-2.1, ПК-2.2, ПК-4.1, ПК-4.2
2.2 Методика PCI. NIST 800-115. Фреймворки для проведения тестирования безопасности ИТ		2		3	5	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	семинарское занятие	ПК-2.1, ПК-2.2, ПК-4.1, ПК-4.2
Итого по разделу		5		6	11			
3. Получение информации о ИТ автоматизированной системы								
3.1 Получение информации из открытых источников. Использование общих ресурсов. Анализ записей DNS	7	3		3	6	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	семинарское занятие	ПК-2.1, ПК-2.2, ПК-4.1, ПК-4.2
3.2 Получение сведений о сетевой маршрутизации. Автоматические инструменты для получения footprint и сбора информации.		3		3	6,4	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	семинарское занятие	ПК-2.1, ПК-2.2, ПК-4.1, ПК-4.2
Итого по разделу		6		6	12,4			

4. Тестирование ИТ автоматизированной системы								
4.1 Идентификация целевого сервиса. Выявление активных сетевых приложений.	7	2		2	6,8	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	семинарское занятие	ПК-2.1, ПК-2.2, ПК-4.1, ПК-4.2
4.2 Средства автоматического тестирования. Nmap, Netdiscover, stricker.		2,5		3	7	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	семинарское занятие	ПК-2.1, ПК-2.2, ПК-4.1, ПК-4.2
Итого по разделу		4,5		5	13,8			
5. Исследование уязвимостей безопасностей ИТ								
5.1 Типы уязвимостей. Классификация уязвимостей.	7	3		2	5	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	семинарское занятие	ПК-2.1, ПК-2.2, ПК-4.1, ПК-4.2
5.2 Автоматическое тестирование уязвимостей ИТ автоматизированной системы. Исследование уязвимостей.		3,5		3	6	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	семинарское занятие	ПК-2.1, ПК-2.2, ПК-4.1, ПК-4.2
Итого по разделу		6,5		5	11			

6. Создание отчетов о тестировании уязвимостей безопасности ИТ								
6.1 Тивы отчетов. Отчет о тестировании безопасности сети.	7	3		3	6	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	семинарское занятие	ПК-2.1, ПК-2.2, ПК-4.1, ПК-4.2
6.2 Автоматизированные системы генерации отчетов. Dradis. Faraday.		3,5		3	8	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	семинарское занятие	ПК-2.1, ПК-2.2, ПК-4.1, ПК-4.2
Итого по разделу		6,5		6	14			
7. Зачет с оценкой								
7.1 Зачет с оценкой	7					Подготовка к зачету с оценкой	Зачет с оценкой	ПК-2.1, ПК-2.2, ПК-4.1, ПК-4.2
Итого по разделу								
Итого за семестр		34		34	74,2		зао	
Итого по дисциплине		34		34	74,2		зачет с оценкой	

5 Образовательные технологии

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

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

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

Формы учебных занятий с использованием традиционных технологий:

• обзорные лекции – для рассмотрения общих вопросов Информатики и информационных технологий, для систематизации и закрепления знаний;

• информационные – для ознакомления с техническими средствами реализации информационных процессов, со стандартами организации сетей, основными приемами защиты информации, и другой справочной информацией;

• лекции-визуализации – для наглядного представления способов решения алгоритмических и функциональных задач, визуализации результатов решения задач;

• Семинар.

• Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму.

Формы учебных занятий с использованием технологий проблемного обучения:

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, автор-ские комментарии, связанные с различными моделями интерпретации изучаемого ма-териала

проблемная - для развития исследовательских навыков и изучения способов ре-шения задач.

лекции с заранее запланированными ошибками – направленные на поиск обучающимися синтаксических и алгоритмических ошибок при решении алгоритмических и функциональных задач, с последующей диагностикой слушателей и разбором сделанных ошибок.

Практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от обучающегося применения как научно-теоретических знаний, так и практических навыков.

Практическое занятие на основе кейс-метода – обучение в контексте моделируемой ситуации, воспроизводящей реальные условия научной, производственной, обще-ственной деятельности. Обучающиеся должны проанализировать ситуацию, разобрать-ся в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации

Формы учебных занятий с использованием игровых технологий:

Учебная игра – форма воссоздания предметного и социального содержания будущей профессиональной деятельности специалиста, моделирования таких систем от-ношений, которые характерны для этой деятельности как целого.

Деловая игра – моделирование различных ситуаций, связанных с выработкой и принятием совместных решений, обсуждением вопросов в режиме «мозгового штурма»

Творческий проект – учебно-познавательная деятельность обучающихся осу-ществляется в рамках рамочного задания, подчиняясь логике и интересам участников проекта, жанру конечного результата (газета, фильм, праздник, издание, экскурсия, подготовка заданий конкурсов и т.п.).

Информационный проект – учебно-познавательная деятельность с ярко выражен-ной эвристической направленностью (поиск, отбор и систематизация информации о каком-то объекте, ознакомление участников проекта с этой информацией, ее анализ и обобщение для презентации более широкой аудитории).

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 (модуля)

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

2. Душкин, А. В. Методологические основы построения защищенных автоматизированных систем: Монография / Душкин А.В. - Воронеж:Научная книга, 2016. - 76 с. ISBN 978-5-4446-0902-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/923295

б) Дополнительная литература:

Ковалев, Д. В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/997105

в) Методические указания:

Баранкова И. И. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности [Электронный ресурс] : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3323.pdf&show=dcatalogues/1/1138331/3323.pdf&view=true (дата обращения: 22.02.2023). - Макрообъект*. - ISBN 978-5-9967-1031-7. - Текст : электронный. - Сведения доступны также на CD-ROM.

3. Методические указания по выполнению практических работ представлены в приложение 3

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронного каталога https://magtu.informsystema.ru .
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта*.

*При открытии макрообъектов учитывайте настройки антивирусной защиты

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	бессрочно
Oracle Virtual Box	свободно распространяемое ПО	бессрочно
Anaconda	свободно	бессрочно
Atom Editor	свободно	бессрочно
NotePad++	свободно	бессрочно
MS Visual Studio Code	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно	бессрочно
Git	свободно	бессрочно
FAR Manager	свободно	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Информационная система - Банк данных угроз безопасности	https://bdu.fstec.ru/
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и	https://fstec.ru/dokumenty-filter
Архив научных журналов «Национальный электронно-информационный	https://archive.neicon.ru/xmlui/
Международная реферативная и полнотекстовая справочная база данных научных изданий «Springer	https://www.nature.com/siteindex
Международная база полнотекстовых журналов Springer Journals	http://link.springer.com/
Университетская информационная система РОССИЯ	https://uisrussia.msu.ru
Федеральный образовательный портал – Экономика. Социология.	http://ecsocman.hse.ru/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	https://magtu.informsystema.ru/Marc.html?locale=ru
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной	URL: http://www1.fips.ru/
Информационная система - Единое окно доступа к информационным	URL: http://window.edu.ru/

Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.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/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:
Материально-техническое обеспечение дисциплины включает:
Лекционная аудитории:
Мультимедийные средства хранения, передачи и представления информации.
Компьютерный класс:
Персональные компьютеры с установленным ПО.
Аудитории для самостоятельной работы
Персональные компьютеры с установленным ПО.

Приложение 1

По дисциплине «Анализ безопасности информационных технологий» 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 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.

Примерный индивидуальные домашние задания

Модуль 1.

1. Какие платформы виртуализации мы можем использовать для создания виртуальных машин?

2. Для чего предназначен файл с .расширением vmdk?

3. Какие логин и пароль используются по умолчанию для входа в Metasploitable.2?

4.Какое дополнительное программное обеспечение потребуется для сборки сервера Metasploitable 3 с нуля?

5. Какая команда используется в Kali Linux для установки нового или обновления существующего пакета?

6. Какая команда применяется для запуска сервиса MySQL?

7. Какая команда используется для запуска сервиса SSH?

Модуль 2.

1.Что означает аббревиатура OSINT?

2. Какие инструменты можно использовать для запроса информации о регистрации домена?

3. Что представляет собой запись A?

4. Какой инструмент использует поисковая система Google для сбора метаданных документов в целевом домене?

5. Какие два автоматизированных инструмента сбора информации наиболее часто используются?

6. Какой инструмент можно применять для поиска информации об устройствах, подключенных к Интернету?

Модуль 6

1. Каковы три основных типа отчетов, представляемых клиентам, о тестировании на проникновение?

2. Какие значения отражает матрица рисков в исполнительном докладе?

3. В чем назначение карты уязвимостей?

Приложение 2

ПК-2: Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей
ПК-2.1: Разрабатывает профили защиты компьютерных систем
Укажите минимальные аппаратные требования к испытательной лаборатории Какие платформы виртуализации мы можем использовать для создания виртуальных машин? Какое дополнительное программное обеспечение потребуется для сборки сервера Metasploitable 3 с нуля? Какой тип анализа безопасности применяется перед вводом в эксплуатацию ИТ ресурсов? Укажите порядок действий при проведении тестирования по стандарту NIST 800-115 При помощи средств виртуальной машины Kali Linux исследовать заданную уязвимость, сформировать отчет. При помощи MSFConsole выполнить автоматизированное исследование тестового информационно-технологического ресурса автоматизированной системы
ПК-2.2: Формирует политики безопасности компьютерных систем и сетей
Создать виртуальную машину Kali Linux Установить Metasploitable 3. Установить apache Выполнить сканирование заданного сайта при помощи Deepmagic Information Gathering Tool. Получить информацию о целевом домене при помощи host и dig Выполнить сканирование заданного сайта при помощиMaltego.
ПК-4: Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей
ПК-4.1: Применяет инструментальные средства проведения мониторинга защищенности компьютерных систем
Используя Nmap выполнить сканирование сети с целью определения конфигурации сети. Используя Nmap выполнить сканирование портов виртуальной маши. Используя Nmap определить установленное сетевое ПО на виртуальной машине Укажите основные типы отчетов. Перечислите основные пункты общего отчета. При помощи Dradis выполнить тестирование безопасности по методологии OWASP и сгенерировать автоматический отчет. Перечислить инструменты для выполнения сканирования уязвимостей доступные в виртуальной машине Kali Linux При помощи ПО Nessus 7 выполнить сканирование уязвимостей целевой автоматизированной системе.
ПК-4.2: Применяет методы анализа защищенности компьютерных систем и сетей
Перечислите источники для получения OSINT информации. При помощи какой утилиты возможно получить информацию о домене DNS. Укажите специализированное ПО необходимое для получения OSINT информации в автоматизированном режиме. Укажите основные категории уязвимостей Приведите пример локальной уязвимости. Приведите приме эксплуатационной уязвимости. Перечислите основные стандарты систематизации уязвимостей.

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 зачета и экзамена.

Критерии оценки для получения зачета с оценкой:

– на оценку «отлично» (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку «хорошо» (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку «удовлетворительно» (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации

«не зачтено» – результат обучения не достигнут, обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач, не может показать знания на уровне воспроизведения и объяснения информации.

Приложение 3

Методические указания по выполнению практических работ

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

Практическое 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 практических навыков решения типовых и прикладных задач.

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

Основными задачами практических занятий являются:

углубление уровня освоения общекультурных и профессиональных компетенций;

обобщение, систематизация, углубление, закрепление полученных практических знаний по конкретным темам дисциплин различных циклов;

приобретение студентами умений и навыков использования современных теоретических знаний в решении конкретных практических задач;

развитие профессионального мышления, профессиональной и познавательной мотивации.

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

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

На практическом 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. Практические работы проводятся под наблюдением преподавателя. К выполнению практических 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 практических работ

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

Практическая работа выполняется каждым студентом самостоятельно, согласно индивидуальному заданию.

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

После выполнения каждой практической работы студент 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 практической 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 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 студент не может исправить даже по требованию преподавателя, или работа не выполнена.