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)

УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ

Направление подготовки (специальность)
20.03.01 Техносферная безопасность

Направленность (профиль/специализация) программы
Управление экологической и промышленной безопасностью

Уровень высшего образования - бакалавриат

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	4
Семестр	7

Магнитогорск
2026 год

Рабочая программа составлена на основе ФГОС ВО - бакалавриат по направлению подготовки 20.03.01 Техносферная безопасность (приказ Минобрнауки России от 25.05.2020 г. № 680)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией
03.02.2026 г. протокол № 5

Председатель _____ В. Р. Храмшин

Согласовано:
Зав. кафедрой Промышленной экологии и безопасности жизнедеятельности

_____ Ю.В. Сомова

Рабочая программа составлена:
ст. преподаватель кафедры ИиИБ, _____ Ю.А. Мазнина

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

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 _____

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 _____

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 _____

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 _____

1 Цели освоения дисциплины (модуля)

1) определение и оценка угроз, разработка моделей угроз в ходе создания и эксплуатации информационных систем;

2) выявление, анализ и устранение уязвимостей в ходе создания и эксплуатации

3) выявление источников угроз несанкционированного доступа (НСД)

4) определение типа нарушителя

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Угрозы кибербезопасности входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

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

Цифровая грамотность

Структура и организация корпоративных информационных систем

Основы программирования на Python

Основы ООП и MVC на Python

Базы данных. SQL-инъекции

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

Пентест

Подготовка к сдаче и сдача государственного экзамена

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

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

Код индикатора	Индикатор достижения компетенции
ДПК-004-5 Способен обеспечить функционирование средств защиты информации в информационно-аналитических системах	
ДПК-004-5.1	Применяет знания в области безопасности вычислительных сетей в информационных системах
ДПК-004-5.2	Применяет знания в организации мер по защите информации в процессе эксплуатации информационных системах

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 акад. часов, в том числе:

– контактная работа – 36,1 акад. часов:

– аудиторная – 36 акад. часов;

– внеаудиторная – 0,1 акад. часов;

– самостоятельная работа – 71,9 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. Нормативные и правовые акты в области защиты информации								
1.1 Основные понятия и задачи моделирования угроз кибербезопасности. База данных угроз ФСТЭК РФ.	7			4	2	Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме.	Текущий контроль успеваемости: – устный опрос (собеседование); – семинарские занятия;	ДПК-004-5.2
Итого по разделу				4	2			
2. Этапы моделирования угроз ИБ								
2.1 Выявление объектов информационной системы, подлежащих защите. Определение источников угроз	7			4	6	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – контрольные работы; – проверка индивидуальных заданий	ДПК-004-5.1, ДПК-004-5.2
2.2 Наиболее часто реализуемые угрозы. Выявление способов				4	20	Подготовка к практическому занятию.	Текущий контроль успеваемости:	ДПК-004-5.1, ДПК-004-5.2

реализации угроз						Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы; – проверка индивидуальных заданий	
2.3 Угрозы мобильным устройствам.	7			4	10,9	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ДПК-004-5.1, ДПК-004-5.2
Итого по разделу				12	36,9			
3. Модель угроз ИСПДн информационной системы персональных данных								
3.1 Угрозы безопасности ПДн. Каналы реализации угроз безопасности ПДн.	7			8	17	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ДПК-004-5.1, ДПК-004-5.2
3.2 Классификация угроз безопасности персональных данных по способу реализации				6	10	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ДПК-004-5.1, ДПК-004-5.2
Итого по разделу				14	27			

4. Методики построения дерева угроз								
4.1 Разработка модели информационной безопасности с учетом реализованных защитных мер. Формирование перечня активов, определение их значимости для компании	7			6	6	Подготовка к практическому занятию. Самостоятельное изучение учебной и научной литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	Текущий контроль успеваемости: – проверка индивидуальных заданий	ДПК-004-5.1, ДПК-004-5.2
Итого по разделу				6	6			
Итого за семестр				36	71,9		зачёт	
Итого по дисциплине				36	71,9		зачет	

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 : учебник для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584050 (дата обращения: 10.03.2026).

2. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 4-е изд. — Москва : РИОР : ИНФРА-М, 2026. — 398 с. — (Высшее образование). — DOI: https://doi.org/10.29039/ 03014-1. - ISBN 978-5-369-

03014-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2242341 (дата обращения: 10.03.2026). – Режим доступа: по подписке.

3. 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: 10.03.2026.

4. Противодействие преступлениям, совершаемым в сфере информационных технологий : учебник / под науч. ред. И.А. Калиниченко. — Москва : ИНФРА-М, 2024. — 642 с. — (Высшее образование: Специалитет). — ISBN 978-5-16-017838-7. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2121606 (дата обращения: 10.03.2026). – Режим доступа: по подписке.

б) Дополнительная литература:

1. Обеспечение безопасности персональных данных [Электронный ресурс]. Национальный открытый университет «Интуит»/.- Режим доступа: https://intuit.ru/studies/courses/697/553/info.- Заглавие с экрана.

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://znanium.ru/catalog/product/997108 (дата обращения: 08.04.2026). – Режим доступа: по подписке.

в) Методические указания:

Методические указания по выполнению практических работ представлены в приложении 3.

Методические указания по выполнению внеаудиторных самостоятельных работ представлены в приложении 4.

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
LibreOffice	свободно распространяемое ПО	бессрочно
MS Office 2003 Professional	№ 135 от 17.09.2007	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp

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:

Лекционные аудитории:

- Мультимедийные средства хранения, передачи и представления информации.

Учебные аудитории для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации:

- 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

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

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде чтения литературы по соответствующему разделу с проработкой материала и выполнения домашних заданий с консультациями преподавателя, а так же с применением кейс-технологий.

а) Контрольные вопросы и задания для проведения текущего контроля

1. Что такое кибербезопасность и почему она важна?
2. Какие основные цели преследуют злоумышленники в киберпространстве?
3. Какие существуют основные принципы обеспечения кибербезопасности?
4. Опишите основные категории угроз кибербезопасности.
5. Что такое уязвимость, угроза и риск в контексте кибербезопасности?
6. Какие существуют этапы жизненного цикла угрозы?
7. Объясните разницу между активными и пассивными атаками.
8. Какие основные методы защиты информации используются для противодействия угрозам?
9. Что такое политика безопасности и какова ее роль в обеспечении кибербезопасности?
10. Какие существуют основные международные и национальные стандарты в области кибербезопасности?
11. Какие основные типы средств защиты информации используются в информационно-аналитических системах?
12. Каковы основные функции межсетевого экрана (firewall)? Какие типы межсетевых экранов существуют?
13. Что такое система обнаружения вторжений (IDS) и как она работает? Какие типы IDS существуют?
14. Что такое система предотвращения вторжений (IPS) и чем она отличается от IDS?
15. Опишите принципы работы антивирусного программного обеспечения.
16. Что такое SIEM (Security Information and Event Management) система и какова ее роль в обеспечении кибербезопасности?
17. Каковы основные принципы работы систем контроля доступа? Какие модели контроля доступа существуют?
18. Что такое шифрование и для чего оно используется? Какие алгоритмы шифрования вы знаете?
19. Объясните принципы работы VPN (Virtual Private Network).
20. Что такое двухфакторная аутентификация и почему она важна?
21. Опишите основные типы сетевых атак (например, DDoS, MITM, sniffing).
22. Что такое сканирование портов и как оно используется злоумышленниками?
23. Объясните, как работает протокол TCP/IP и какие уязвимости могут быть связаны с его использованием.
24. Что такое DNS-спуфинг и как от него защититься?
25. Какие существуют методы защиты беспроводных сетей (Wi-Fi)?
26. Опишите основные принципы построения безопасной сетевой архитектуры.
27. Что такое сегментация сети и зачем она нужна?
28. Какие инструменты используются для мониторинга сетевого трафика и обнаружения аномалий?

29. Каковы основные этапы управления рисками в кибербезопасности?
30. Опишите основные меры по обеспечению физической безопасности информационных систем.
31. Какова роль обучения и повышения осведомленности пользователей в области кибербезопасности?
32. Какие процедуры необходимо выполнять при обнаружении инцидента кибербезопасности?
33. Что такое план восстановления после аварии (Disaster Recovery Plan) и какова его цель?
34. Как обеспечить безопасность облачных сред?
35. Что такое тестирование на проникновение (пентест) и как оно используется для оценки уровня безопасности ИС?
36. Как обеспечить безопасность веб-приложений? Какие типы уязвимостей веб-приложений наиболее распространены?
37. Как обеспечить безопасность баз данных?
38. Что такое аудит безопасности и как он проводится?
39. Как обеспечить соответствие требованиям регуляторов в области кибербезопасности?
40. Что такое управление уязвимостями и как оно осуществляется?

б) Примеры индивидуальных домашних заданий

1. Используя Nmap, проведите сканирование заданной сети и определите открытые порты, работающие службы и операционные системы хостов. Сформируйте отчет о результатах сканирования.
2. Настройте заданный межсетевой экран для защиты заданной системы. Разрешите только необходимые соединения и заблокируйте все остальные, сформируйте скрипт. Составьте отчет о проделанной работе с с описанием правил и обоснованием их необходимости.
3. Используя сканер уязвимостей Nessus (или OpenVAS), проведите сканирование заданной системы и определите имеющиеся уязвимости. Сформируйте отчет о результатах сканирования с указанием обнаруженных уязвимостей, их уровня опасности и рекомендаций по устранению.
4. Настройте web application firewall для защиты заданного веб-приложения от распространенных атак. Составьте отчет о проделанной работе, описав правила конфигурации и их назначение.

Приложение 2

Оценочные средства для проведения промежуточной аттестации

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

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ДПК-004-5 Способен обеспечить функционирование средств защиты информации в информационно-аналитических системах – ДПК-004-5.1 Применяет знания в области безопасности вычислительных сетей в информационных системах – ДПК-004-5.2 Применяет знания в организации мер по защите информации в процессе эксплуатации информационных системах		
ДПК-004-5.1	Применяет знания в области безопасности вычислительных сетей в информационных системах	Теоретические вопросы к зачету: 1. Что такое кибербезопасность и почему она важна? 2. Какие основные цели преследуют злоумышленники в киберпространстве? 3. Какие существуют основные принципы обеспечения кибербезопасности? 4. Опишите основные категории угроз кибербезопасности. 5. Что такое уязвимость, угроза и риск в контексте кибербезопасности? 6. Какие существуют этапы жизненного цикла угрозы? 7. Объясните разницу между активными и пассивными атаками. 8. Какие основные методы защиты информации используются для противодействия угрозам? 9. Что такое политика безопасности и какова ее роль в обеспечении кибербезопасности? 10. Какие существуют основные международные и национальные стандарты в области кибербезопасности? 11. Какие основные типы средств защиты информации используются в информационно-аналитических системах? 12. Каковы основные функции межсетевого экрана (firewall)? Какие типы межсетевых экранов существуют? 13. Что такое система обнаружения вторжений (IDS) и как она работает? Какие типы IDS существуют? 14. Что такое система предотвращения вторжений (IPS) и чем она отличается от IDS? 15. Опишите принципы работы антивирусного программного обеспечения. 16. Что такое SIEM (Security Information and Event Management) система и какова ее роль в обеспечении кибербезопасности? 17. Каковы основные принципы работы систем контроля доступа? Какие модели контроля доступа существуют?

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		18. Что такое шифрование и для чего оно используется? Какие алгоритмы шифрования вы знаете? 19. Объясните принципы работы VPN (Virtual Private Network). 20. Что такое двухфакторная аутентификация и почему она важна? 21. Опишите основные типы сетевых атак (например, DDoS, MITM, sniffing). 22. Что такое сканирование портов и как оно используется злоумышленниками? 23. Объясните, как работает протокол TCP/IP и какие уязвимости могут быть связаны с его использованием. 24. Что такое DNS-спуфинг и как от него защититься? 25. Какие существуют методы защиты беспроводных сетей (Wi-Fi)? 26. Опишите основные принципы построения безопасной сетевой архитектуры. 27. Что такое сегментация сети и зачем она нужна? 28. Какие инструменты используются для мониторинга сетевого трафика и обнаружения аномалий? Примеры практических заданий для зачета: 1. С помощью программы-анализатора трафика для компьютерных сетей Wireshark перехватите и проанализируйте сетевой трафик. Определите типы протоколов, используемых в сети, и выявите потенциально опасные соединения. Сформируйте отчет о результатах анализа. 2. Проанализируйте лог-файлы веб-сервера, системы контроля доступа или межсетевого экрана. Выявите подозрительные события и попытки несанкционированного доступа. Сформируйте отчет о проделанной работе с описанием выявленных подозрительных событий, их возможными последствиями и рекомендациями по защите.
ДПК-004-5.2	Применяет знания в организации мер по защите информации в процессе эксплуатации информационных системах	Теоретические вопросы к зачету: 1. Каковы основные этапы управления рисками в кибербезопасности? 2. Опишите основные меры по обеспечению физической безопасности информационных систем. 3. Какова роль обучения и повышения осведомленности пользователей в области кибербезопасности? 4. Какие процедуры необходимо выполнять при обнаружении инцидента кибербезопасности? 5. Что такое план восстановления после аварии (Disaster Recovery Plan) и какова его цель? 6. Как обеспечить безопасность облачных сред? 7. Что такое тестирование на проникновение (пентест) и как оно используется для оценки уровня

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		безопасности ИС? 8. Как обеспечить безопасность веб-приложений? Какие типы уязвимостей веб-приложений наиболее распространены? 9. Как обеспечить безопасность баз данных? 10. Что такое аудит безопасности и как он проводится? 11. Как обеспечить соответствие требованиям регуляторов в области кибербезопасности? 12. Что такое управление уязвимостями и как оно осуществляется? Примеры практических заданий для зачета: 1. Используя Hydra, проведите bruteforce атаку на заданную службу. Настройте защиту от bruteforce атак. Сформируйте отчет о проделанной работе, описав проведенную bruteforce атаку, оценив эффективность защиты и дав рекомендации по ее усилению. 2. Получите хэш пароля. Подберите пароль, используя различные словари и техники. Оцените стойкость пароля. Составьте отчет о проделанной работе, дав рекомендации по созданию надежных паролей. 3. На основе смоделированного инцидента безопасности создайте отчет об инциденте, включающий описание инцидента, его последствия и принятые меры. 4. Проведите оценку рисков безопасности для заданной информационной системы. Определите активы, угрозы, уязвимости и возможные последствия. Предложите меры по снижению рисков.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания

Показатели и критерии оценивания зачета:

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

− «не зачтено» – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

Приложение 3

Методические указания по выполнению практических работ

Практические работы проводятся в компьютерных классах целью получения практических умений для формирования и развития профессиональных навыков и соответствующих компетенций по дисциплине. При подготовке к выполнению заданий практической работы используйте лекции, справочный материал программного обеспечения, рекомендованную литературу и цифровые образовательные ресурсы соответствующих методических материалов, размещенных в сети Интернет или локальной сети университета. Перед выполнением практической работы необходимо получить свой вариант индивидуального задания у преподавателя. Прежде чем приступить к выполнению практической работы, внимательно прочтите рекомендации к ее выполнению. Ознакомьтесь с перечнем рекомендуемой литературы, повторите теоретический материал, относящийся к теме работы. Ответьте на контрольные вопросы, выполните задания для самостоятельного выполнения. По результатам практической работы предоставляется отчет. Отчет к практическим работам должен содержать:

- название практической работы;
- цель и задачи работы;
- краткие теоретические сведения;
- задания по практической работе;
- ход работы - описание последовательности действий при выполнении работы;
- выводы или результаты.

Результаты выполнения практической работы могут быть представлены в электронном варианте или распечатанные. Результаты выполнения заданий практической работы можно сохранить на образовательном портале в личном кабинете и использовать при подготовке к экзамену.

Защита работы и результаты оценивания

Защита проводится в два этапа:

1. Демонстрируются результаты выполнения задания. В случае выполнения практической работы, предусматривающей разработку программы, при помощи тестового примера доказывается, что результат, получаемый при выполнении программы, является правильным.

2. Для защиты работы студенту необходимо ответить на дополнительные вопросы преподавателя. Каждая практическая работа оценивается определенным количеством баллов исходя из 5-бальной системы оценок.

Практическая работа считается выполненной и защищенной, если выполнены все задания и даны правильные ответы преподавателю на заданные вопросы. Практическая работа считается выполненной и незащищенной, если выполнены все задания, но полученные результаты являются неверными или не даны правильные ответы преподавателю на заданные вопросы и ответы были не полные. Обучающемуся, не выполнившим в полном объеме все задания практической работы, или пропустившим по уважительной причине практическую работу, необходимо выполнить ее самостоятельно в компьютерном классе, результаты выполненной работы сохранить на съемном накопителе или на образовательном портале. Результаты предоставить в сроки, указанные преподавателем вместе с отчетом, демонстрацией полученных результатов в компьютерном классе или предоставлением материалов на электронном образовательном ресурсе.

Правила по технике безопасности для обучающихся
при проведении практических работ

1. Практические работы проводятся под наблюдением преподавателя. К выполнению практических работ студенты допускаются только после прослушивания инструктажа по технике безопасности и противопожарным мерам.

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

Приложение 4

Методические указания по выполнению внеаудиторных самостоятельных работ

Общие положения

Настоящие методические указания предназначены для организации внеаудиторной самостоятельной работы студентов 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):
   - предоставляемыми преподавателем на лекционных занятиях;
   - предоставляемыми преподавателем в рамках электронных образовательных курсов;
   - 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 со студентами 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 приложении 2 данной РПД.