



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)

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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	2
Семестр	3

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:
ст. преподаватель кафедры ИиИБ,

 М.В.Афанасьева

Рецензент:
Начальник отдела информационной безопасности "КУБ" (АО),

 М.М. Блинецов

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)

Целью дисциплины «Основы информационной безопасности» является понимание социальной значимости своей будущей профессии в соответствии с доктриной информационной безопасности Российской Федерации. Формирование у студентов навыков их практического применения в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем». Дисциплина «Основы информационной безопасности» рассматривает основные принципы и основные направления обеспечения информационной безопасности Российской Федерации.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Основы информационной безопасности входит в обязательную часть учебного плана образовательной программы.

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

Основы безопасности цифрового общества

Информатика

Физика

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

Анализ рисков информационной безопасности

Безопасность Интернета вещей

Безопасность сетей ЭВМ

Безопасность операционных систем

Методы и средства криптографической защиты информации

Методы выявления нарушений информационной безопасности

Методы и стандарты оценки защищенности компьютерных систем

Методы проектирования систем защиты распределенных информационных систем

Моделирование угроз информационной безопасности

Организационное и правовое обеспечение информационной безопасности

Обеспечение информационной безопасности критической информационной инфраструктурой

Программно-аппаратные средства обеспечения информационной безопасности

Управление информационной безопасностью

Технология построения защищенных распределенных приложений

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

В результате освоения дисциплины (модуля) «Основы информационной безопасности» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ОПК-9	Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;
ОПК-9.1	Использует технические средства защиты информации
ОПК-9.2	Применяет современные средства защиты сетей и систем защиты информации

4. Структура, объём и содержание дисциплины (модуля)

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

- контактная работа – 73,9 акад. часов;
- аудиторная – 72 акад. часов;
- внеаудиторная – 1,9 акад. часов;
- самостоятельная работа – 70,1 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. Место и роль информационной безопасности в системе национальной безопасности РФ								
1.1 Сущность и понятие информации. Понятие национальной безопасности. Законодательный уровень ИБ. Ответственность за нарушение ИБ.	3	4	4/И		6	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к контрольному тестированию и устному опросу.	Устный опрос, контрольное тестирование	ОПК-9.1, ОПК-9.2
1.2 Угрозы безопасности информации, осуществляемые через информационную среду. Коммерческая тайна.		4	4/И		6	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к контрольному тестированию и устному опросу.	Устный опрос, контрольное тестирование	ОПК-9.1, ОПК-9.2
Итого по разделу		8	8/И		12			
2. Классификация защищаемой информации и угроз информационной безопасности								

2.1 Классификация защищаемой информации по видам тайны и степеням конфиденциальности. Государственная тайна.	3	4	4/ИИ		6	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к индивидуальному домашнему заданию (ИДЗ). Подготовка к аудиторной контрольной работе (АКР).	ИДЗ, АКР	ОПК-9.1, ОПК-9.2
2.2 Источники и классификация угроз информационной безопасности для объектов информатизации. Оранжевая книга.		4			6	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к рубежному контролю.	Рубежный контроль в форме аудиторной контрольной работы	ОПК-9.1, ОПК-9.2
Итого по разделу		8	4/ИИ		12			
3. Способы обеспечения информационной безопасности автоматизированных систем								
3.1 Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации. Построение модели IDEF0.	3	8	12/ИИ		20	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к индивидуальному домашнему заданию (ИДЗ).	ИДЗ	ОПК-9.1, ОПК-9.2
3.2 Классификация средств и способов обеспечения информационной безопасности, принципы построения систем защиты информации. Построение модели IDEF3.		4	4/ИИ		8	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к индивидуальному домашнему	ИДЗ, АКР	ОПК-9.1, ОПК-9.2

						заданию (ИДЗ). Подготовка к аудиторной контрольной работе (АКР).		
Итого по разделу		12	16/2И		28			
4. Методы формирования требований по защите информации								
4.1 Анализ существующих методов и средств, применяемых для защиты информации.	3	4	4/1,3И		6	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка презентаций для защиты докладов.	Доклад по практической работе	ОПК-9.1, ОПК-9.2
4.2 Разработка предложений по совершенствованию существующих методов и средств, применяемых для контроля и защиты информации и повышению их эффективности		4	4		6	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к рубежному контролю.	Рубежный контроль в форме тестирования	ОПК-9.1, ОПК-9.2
4.3 Подготовка к зачету					6,1	Самостоятельное изучение учебной и научно литературы, работа с материалами образовательного портала и ЭБС. Подготовка к зачету.	Зачет	ОПК-9.1, ОПК-9.2
Итого по разделу		8	8/1,3И		18,1			
Итого за семестр		36	36/6,3 И		70,1		зачёт	
Итого по дисциплине		36	36/6,3 И		70,1		зачет	

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины 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, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/490277> (дата обращения: 11.03.2026).

2. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2024. — 400 с. — (Высшее образование). — DOI: <https://doi.org/10.12737/1759-3>. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: <https://znanium.ru/catalog/product/2140566> (дата обращения: 11.03.2026). – Режим доступа: по подписке.

б) Дополнительная литература:

1. 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> (дата обращения: 13.03.2026).

2. Внуков, А. А. Защита информации в банковских системах : учебник для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2026. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/584051> (дата обращения: 13.03.2026).

3. Определение критически значимых ресурсов объекта защиты при составлении модели угроз информационной безопасности : учебное пособие / И. И. Баранкова, О. В. Пермякова ; МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). - URL: <https://host.megaprolib.net/MP0109/Download/MObject/1858> (дата обращения: 13.03.2026). - ISBN 978-5-9967-1031-7. - Текст : электронный*.

в) Методические указания:

1. Методические указания по выполнению практических работ (Приложение 3).
2. Методические указания по выполнению внеаудиторных самостоятельных работ (Приложение 4).

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
7Zip	свободно распространяемое ПО	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
MS Visual Studio Code	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно
Calculate Linux Desktop Xfce	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/?ysclid=lujkqy7cnw630508962
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

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Материально-техническое обеспечение дисциплины включает:

Лекционные аудитории:

- Мультимедийные средства хранения, передачи и представления информации.

Компьютерные классы:

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

Помещения для самостоятельной работы обучающихся:

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

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

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

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

Рубежный контроль осуществляется в виде проведения промежуточной аттестации по разделу с целью определения успеваемости обучающихся и осуществляется под контролем преподавателя в виде решения задач, выполнения упражнений и прохождения тестирований, которые определяет преподаватель для студента с использованием *методов ИТ*.

Задания и вопросы по темам

Тема 1. Законодательный уровень ИБ. Ответственность за нарушение ИБ.

Вопросы:

1. Федеральный закон «Об информации, информационных технологиях и о защите информации»
2. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации
3. Право на доступ к информации
4. Ограничение доступа к информации
5. Распространение информации или предоставление информации
6. Документирование информации. Государственное регулирование в сфере применения информационных технологий
7. Информационные системы. Государственные информационные системы
8. Использование информационно-телекоммуникационных сетей
9. Защита информации
10. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации

Тема 2. Коммерческая тайна.

Вопросы:

1. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ. Цели, сфера действия и основные понятия федерального закона
2. Право на отнесение информации к информации, составляющей коммерческую тайну, и способы получения такой информации
3. Сведения, которые не могут составлять коммерческую тайну
4. Предоставление информации, составляющей коммерческую тайну. Права обладателя информации, составляющей коммерческую тайну
5. Охрана конфиденциальности информации
6. Охрана конфиденциальности информации при ее предоставлении
7. Охрана конфиденциальности информации, составляющей коммерческую тайну, в рамках трудовых отношений
8. Ответственность за нарушение настоящего Федерального закона о коммерческой тайне
9. Ответственность за непредоставление органам государственной власти, иным государственным органам, органам местного самоуправления информации, составляющей коммерческую тайну

Тема 3. Государственная тайна.

1. Закон РФ от 21 июля 1993 г. N 5485-1 "О государственной тайне" (с изменениями и дополнениями). Общие Положения
2. Перечень сведений, составляющих государственную тайну
3. Принципы отнесения сведений к государственной тайне и засекречивания этих сведений. Степени секретности сведений и грифы секретности носителей этих сведений
4. Порядок отнесения сведений к государственной тайне. Сведения, не подлежащие отнесению к государственной тайне и засекречиванию
5. Ограничение прав собственности предприятий, учреждений, организаций и граждан Российской Федерации на информацию в связи с ее засекречиванием. Порядок засекречивания сведений и их носителей. Реквизиты носителей сведений, составляющих государственную тайну
6. Рассекречивание сведений и их носителей.
7. Передача сведений, составляющих государственную тайну.
8. Защита сведений, составляющих государственную тайну, при изменении функций субъектов правоотношений
9. Органы защиты государственной тайны

10. Оформление допуска должностного лица или гражданина к государственной тайне. Обязанности должностных лиц и граждан Российской Федерации, допущенных к государственной тайне, и социальные гарантии. Основания для отказа должностному лицу или гражданину в допуске к государственной тайне. Условия прекращения допуска должностного лица или гражданина к государственной тайне. Ограничения прав должностного лица или гражданина, допущенных или ранее допускавшихся к государственной тайне

11. Организация доступа должностного лица или гражданина к сведениям, составляющим государственную тайну. Ответственность за нарушение законодательства Российской Федерации о государственной тайне. Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну

13. Порядок сертификации средств защиты информации. Финансирование мероприятий по защите государственной тайны

14. Контроль и надзор за обеспечением защиты государственной тайны

Тема 4. Оранжевая книга.

1. Определение классов безопасности
2. Требования к политике безопасности
3. Требования к подотчетности
4. Требования к гарантированности
5. Требования к документации

Темы 5-6. Модели данных.

1. Методология IDEF0
2. Основные элементы IDEF0 и структура функциональной модели
3. Требования к построению модели IDEF0
4. Методология IDEF3
5. Синтаксис и семантика моделей IDEF3
6. Соединение типа "и" в модели IDEF3
7. Соединение типа "или" в модели IDEF3
8. Соединение типа "исключающее "или" в модели IDEF3

Контрольные вопросы и задания для проведения текущего контроля

Темы для ИДЗ:

1. Составить модель данных согласно методологии IDEF0 для объекта
Консалтинговая фирма
2. Составить модель данных согласно методологии IDEF0 для объекта Рекламное
агентство
3. Составить модель данных согласно методологии IDEF0 для объекта
Юридическая фирма
4. Составить модель данных согласно методологии IDEF0 для объекта Адвокатская
контора
5. Составить модель данных согласно методологии IDEF0 для объекта
Клининговая фирма
6. Составить модель данных согласно методологии IDEF0 для объекта Магазин по
сборке и продаже компьютеров
7. Составить модель данных согласно методологии IDEF0 для объекта Детективное
агентство
8. Составить модель данных согласно методологии IDEF0 для объекта
Нотариальная контора
9. Составить модель данных согласно методологии IDEF0 для объекта
Туристическое агентство
10. Составить модель данных согласно методологии IDEF0 для объекта SMM
агентство
11. Составить модель данных согласно методологии IDEF0 для объекта частный
детский сад
12. Составить модель данных согласно методологии IDEF0 для объекта Firma,
оказывающая услуги экспресс доставки
13. Составить модель данных согласно методологии IDEF0 для объекта Firma, по
ремонту бытовой техники
14. Составить модель данных согласно методологии IDEF0 для объекта Агентство
недвижимости (предоставление недвижимости для съема)
15. Составить модель данных согласно методологии IDEF0 для объекта
Риэлтерское агентство
16. Составить модель данных согласно методологии IDEF0 для объекта Ателье.
17. Составить модель данных согласно методологии IDEF0 для объекта Автосервис
18. Составить модель данных согласно методологии IDEF0 для объекта Салон
красоты

19. Составить модель данных согласно методологии IDEF0 для объекта
Бухгалтерская фирма

20. Составить модель данных согласно методологии IDEF0 для объекта
Генеалогический центр

Темы для докладов:

1. Актуальные инструменты ИБ специалиста
2. Реверс инжиниринг
3. Информационные системы. Автоматизированные системы. Типы, различия, основные принципы работы
4. Информационно-техническая война
5. Информационно-психологическая война
6. Кибертерроризм
7. Этические нормы поведения в сети. Кибергигиена
8. Методы борьбы с фишинговыми атаками
9. Борьба со спамом: основные подходы, классификация, примеры
10. Квантовая криптография
11. Утечки информации: как избежать. Безопасность смартфонов
12. Ботнеты - плацдарм современных кибератак
13. Windows и Linux: что безопаснее?
14. Стеганографические методы защиты информации
15. Технология цифровых водяных знаков
16. Компьютерные вирус, их свойства и классификация. Антивирусы
17. Методы сканирования уязвимостей
18. Программные закладки
19. Стратегия развития цифрового общества в России
20. Угрозы национальной безопасности страны в экономической сфере, осуществляемые через информационную среду

ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

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

Код индикатора	Индикатор достижения компетенции	Оценочные средства
ОПК-9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации;		
ОПК-9.1	Использует технические средства защиты информации	<ol style="list-style-type: none"> 1. Составить майнд-карту, связывающая все законы, регламентирующие наказание за нарушение ИБ. 2. Изучить нормативные документы по коммерческой тайне и составить майнд-карту, связывающую эти документы между собой. 3. Изучить нормативные документы по государственной тайне и составить майнд-карту, связывающую эти документы между собой. 4. Уметь определять уровни надежности технических средств защиты информации и требования к ним.
ОПК-9.2	Применяет современные средства защиты сетей и систем защиты информации	<ol style="list-style-type: none"> 1. Разработать инфографику с целью анализа существующих методов и средств, применяемых для защиты информации. 2. На основе проведенного анализа нормативно-правовых документов в области защиты информации автоматизированных систем разработать предложения по совершенствованию системы управления безопасностью информации в автоматизированных системах на современном уровне развития общества. 3. Составить модель данных согласно методологии IDEF0 для заданного объекта 4. Составить модель данных согласно методологии IDEF3 для заданного объекта

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

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.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

Лабораторные работы проводятся в компьютерных классах или специализированных лабораториях с целью получения практических умений для формирования и развития профессиональных навыков и соответствующих компетенций по дисциплине. При подготовке к выполнению заданий лабораторной 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 лабораторной работы необходимо получить свой вариант индивидуального задания у преподавателя. Прежде чем приступить к выполнению лабораторной 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 лабораторной работы предоставляется отчет. Отчет к лабораторным работам должен содержать:

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

Результаты выполнения лабораторной работы могут быть представлены в электронном варианте или распечатанные. Результаты выполнения заданий лабораторной 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 лабораторной работы, предусматривающей разработку программы, при помощи тестового примера доказывається, что результат, получаемый при выполнении программы, является правильным.

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

Лабораторная работа считается выполненной и защищенной, если выполнены все

задания и даны правильные ответы преподавателю на заданные вопросы. Лабораторная 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 выполнившему в полном объеме все задания лабораторной работы, или пропустившим по уважительной причине лабораторную работу, необходимо выполнить ее самостоятельно в компьютерном классе или специализированной лаборатории, 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 специализированной лаборатории) или предоставлением материалов на электронном образовательном ресурсе.

Правила по технике безопасности для обучающихся при проведении лабораторных работ:

1. Лабораторные работы проводятся под наблюдением преподавателя. К выполнению лабораторных 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.

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):

а) предоставляемыми преподавателем на лекционных занятиях;
б) предоставляемыми преподавателем в рамках электронных образовательных курсов;

с) 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, аудиторские 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.