МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

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

УТВЕРЖДАЮ
Директор ИЭиАС
В.Р. Храмшин
04.02.2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

АНАЛИЗ РИСКОВ 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	4
Семестр	8

Магнитогорск
2025 год

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

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

Зав. кафедрой _____ И.И. Баранкова

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

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
зав. кафедрой кафедры ИиИБ, д-р техн. наук _____ И.И. Баранкова

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

Лист актуализации рабочей программы

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

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

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

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

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

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

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

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

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

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

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

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

1 Цели освоения дисциплины (модуля)

Целями освоения дисциплины (модуля) «Анализ рисков информационной безопасности» являются: выявление источников и способов реализации угроз информационной безопасности, фиксация параметров безопасности и анализа безопасности АС, изучение основных понятий и принципов анализа и оценки рисков информационной безопасности.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Анализ рисков информационной безопасности входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

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

Моделирование угроз информационной безопасности

Организационное и правовое обеспечение информационной безопасности

Безопасность операционных систем

Безопасность Интернета вещей

Безопасность сетей ЭВМ

Безопасность систем баз данных

Защита информации от утечки по техническим каналам

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

Подготовка к сдаче и сдача государственного экзамена

Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

Производственная - научно-исследовательская работа

Производственная - преддипломная практика

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

Обеспечение информационной безопасности критической информационной инфраструктурой

Методы проектирования систем защиты распределенных информационных систем

Моделирование систем защиты информации

Управление информационной безопасностью

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

В результате освоения дисциплины (модуля) «Анализ рисков информационной безопасности» 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

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

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. Методики и технологии управления рисками информационной безопасности и их оценки								
1.1 Оценочные стандарты в информационной безопасности. Роль стандартов информационной безопасности. «Критерии определения безопасности компьютерных систем» как оценочный стандарт. Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.	8	4		8	10	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме.	– устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий.	ПК-2.1, ПК-2.2
1.2 Методика оценки рисков информационной безопасности предприятия. Управление рисками. Основные понятия. Метод оценки рисков на основе модели угроз и уязвимостей		6		10/6И	10	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ПК-2.1, ПК-2.2
1.3 Методика оценки рисков информационной		6		6	10	Подготовка к практическому	устный опрос (собеседование);	ПК-2.1, ПК-2.2

организации. Метод оценки рисков на основе модели информационных потоков. Расчет рисков по угрозе конфиденциальность						занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	
1.4 Методики и технологии управления рисками. Качественные методики управления рисками. Количественные методики управления рисками. Метод CRAMM	8	6		3	15	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ПК-2.1, ПК-2.2
1.5 Разработка корпоративной методики анализа рисков. Постановка задачи. Методы оценивания информационных рисков. Табличные методы оценки рисков. Оценка рисков по двум факторам. Разделение рисков на приемлемые и неприемлемые. Оценка рисков по трем факторам. Методика анализа рисков Microsoft		6		3/2,9И	15	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ПК-2.1, ПК-2.2
1.6 Современные методы и средства анализа и управление рисками информационных систем. Методика FRAP. Методика OCTAVE. Методика RiskWatch		6		4/3И	14,2	Подготовка к практическому занятию. Самостоятельное изучение учебной и научно литературы. Работа с электронными библиотеками. Поиск дополнительной информации по заданной теме	– устный опрос (собеседование); – контрольные работы; – семинарские занятия; – проверка индивидуальных заданий	ПК-2.1, ПК-2.2
Итого по разделу		34		34/11,9И	74,2			
Итого за семестр		34		34/11,9И	74,2		зачёт	

Итого по дисциплине	34		34/11,9 И	74,2		зачет	

5 Образовательные технологии

При проведении учебных занятий организация обеспечивает развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

1. Традиционные образовательные технологии ориентируются на организацию образовательного процесса, предполагающую прямую трансляцию знаний от преподавателя к студенту (преимущественно на основе объяснительно-иллюстративных методов обучения). Учебная деятельность студента носит в таких условиях, как правило, репродуктивный характер.

Формы учебных занятий с использованием традиционных технологий:

Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

Семинар – беседа преподавателя и студентов, обсуждение заранее подготовленных сообщений по каждому вопросу плана занятия с единым для всех перечнем рекомендуемой обязательной и дополнительной литературы.

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

Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2. Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности студентов.

Формы учебных занятий с использованием технологий проблемного обучения:

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов, авторские комментарии, связанные с различными моделями интерпретации изучаемого материала.

Лекция «вдвоем» (бинарная лекция) – изложение материала в форме диалогического общения двух преподавателей (например, реконструкция диалога представителей различных научных школ, «ученого» и «практика» и т.п.).

Практическое занятие в форме практикума – организация учебной работы, направленная на решение комплексной учебно-познавательной задачи, требующей от студента 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, общественной деятельности. Обучающиеся должны проанализировать ситуацию, разобраться в сути проблем, предложить возможные решения и выбрать лучшее из них. Кейсы базируются на реальном фактическом материале или же приближены к реальной ситуации.

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. Сетевая защита информации. Лабораторный практикум : учебное пособие [для вузов] / Д. Н. Мазнин, И. И. Баранкова, У. В. Михайлова, М. В. Афанасьева ;

Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г.

И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://host.megaprolib.net/MP0109/Download/MObject/2400. - ISBN 978-5-9967-1605-0. -

Текст : электронный.*МАКРООБЪЕКТ

2. Царегородцев, А. В. Анализ рисков в процессах обеспечения информационной безопасности жизненного цикла финансовых автоматизированных информационных систем : монография / А.В. Царегородцев, С.В. Романовский, С.Д. Волков. — Москва : ИНФРА-М, 2024. — 198 с. — (Научная мысль). — DOI 10.12737/2049718. - ISBN 978-5-16-018719-8. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2049718 (дата обращения: 12.04.2024). – Режим доступа: по подписке.

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронной библиотеки МГТУ им. Г. И. Носова https://host.megaprolib.net/MP0109/Web.

2. Произвести авторизацию на портале (логин: Фамилия на русском языке, пароль: номер читательского билета)

3. Активизировать гиперссылку макрообъекта.

б) Дополнительная литература:

1. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2024. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/2052391 (дата обращения: 12.04.2024). – Режим доступа: по подписке.

2. Михайлова У. В. Безопасность корпоративной инфраструктуры : практикум [для вузов] / У. В. Михайлова, М. В. Афанасьева ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2021. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://host.megaprolib.net/MP0109/Download/MObject/3254. - Текст : электронный. *РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

1. Перейти по адресу электронной библиотеки МГТУ им. Г. И. Носова https://host.megaprolib.net/MP0109/Web.

2. Произвести авторизацию на портале (логин: Фамилия на русском языке, пароль: номер читательского билета)

3. Активизировать гиперссылку макрообъекта.

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
Adobe Reader	свободно распространяемое ПО	бессрочно
Calculate Linux Desktop Xfce	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/
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/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

1) Лаборатория программно-аппаратных средств обеспечения информационной безопасности (2124):

ПЭВМ на базе Windows 10 – 12 шт

2) Лекционная аудитория (ауд. 2124, ауд. 2113, ауд. 365, ауд. 388 и т.д.)- Мультимедийные средства хранения, передачи и представления информации

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

4) Аудитория для самостоятельной работы: читальные залы библиотеки, ауд 132а

ПРИЛОЖЕНИЕ 1

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Перечень тем для подготовки к практическим занятиям:

Тема 1. Основные понятия информационной безопасности

– Понятие информационной безопасности.

– Основные составляющие информационной безопасности.

– Управление информационной безопасностью.

– Важность и сложность проблемы информационной безопасности.

Тема 2. Оценочные стандарты в информационной безопасности.

– Роль стандартов информационной безопасности.

– «Критерии определения безопасности компьютерных систем» как оценочный стандарт.

– Международный стандарт ISO/IEC 15408. Критерии оценки безопасности информационных систем.

Тема 3. Стандарты управления информационной безопасностью.

–Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799.

–Международный стандарт ISO/IEC 27001:2005 "Системы управления информационной безопасности. Требования".

–Сертификация СУИБ на соответствие ISO 27001.

Тема 4. Создание СУИБ на предприятии.

–Этапы разработки и внедрения системы управления ИБ.

–Содержание этапов разработки и внедрения системы управления ИБ.

Тема 5. Методика оценки рисков информационной безопасности предприятия.

–Управление рисками. Основные понятия.

–Метод оценки рисков на основе модели угроз и уязвимостей.

Тема 6. Методика оценки рисков информационной организации.

– Метод оценки рисков на основе модели информационных потоков.

– Расчет рисков по угрозе конфиденциальность.

Тема 7. Методики и технологии управления рисками.

– Качественные методики управления рисками.

– Количественные методики управления рисками. Метод CRAMM.

Тема 8. Разработка корпоративной методики анализа рисков.

– Методы оценивания информационных рисков.

– Табличные методы оценки рисков.

– Оценка рисков по двум факторам.

– Разделение рисков на приемлемые и неприемлемые.

– Оценка рисков по трем факторам.

– Методика анализа рисков Microsoft.

Тема 9 Современные методы и средства анализа и управление рисками информационных систем.

– Методика FRAP.

– Методика OCTAVE.

– Методика RiskWatch.

Перечень контрольных вопросов по терминологии:

Угроза (Threat)

Уязвимость (Vulnerability)

• *Анализ рисков.*

Базовый уровень безопасности .

Базовый (Baseline) анализ рисков .
Полный (Full) анализ рисков.
Риск нарушения ИБ (Security Risk).
Оценка рисков (Risk Assessment).
Управление рисками (Risk Management).
Система управления ИБ (Information Security Management System).
Класс рисков.
Терминология COBIT
• *Риски*
Типы рисков.
Приемлемый уровень риска
Стандарт управления рисками.
Матрица ИТ рисков.
• *Руководство рисками*
Владелец процессов оценки рисков.
План работ по снижению рисков.
Политики и процедуры.
Обновление величин рисков.
Глобальный и системный уровни оценки ИТ- рисков.
Резюме для руководителя.
Стратегия управления ИТ
• *Идентификация*
Определение компонентов риска.
Области рисков.
Обновление матрицы рисков.
Меры оценки
Количественная оценка.
Качественная оценка.
• *Способы управления*
Независимое мнение.
Возврат инвестиций.
Баланс способов управления
Управление конфликтами.
• *Мониторинг*
Мониторинг используемых способов управления.
Процедура реагирования на инциденты.
Согласование плана работ по снижению рисков.

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
ПК-2 Способен разрабатывать требования по защите, формировать политики безопасности компьютерных систем и сетей		
ПК-2.1	Разрабатывает профили защиты компьютерных систем	1. Методика оценки рисков информационной безопасности компании. 2. Управление рисками. Перечислить основные понятия. 3. Метод оценки рисков на основе модели угроз и уязвимостей. 4. Расчет рисков по угрозе информационной безопасности. 5. Метод оценки рисков на основе модели информационных потоков. Задание: Провести расчеты оценки рисков информационной безопасности компании по методу оценки рисков на основе частной модели угроз.
ПК-2.2	Формирует политики безопасности компьютерных систем и сетей	***Задание*** Для заданного предприятия разработать: – карту информационных активов фирмы; – карты уязвимостей и угроз; – отчет о результатах оценки рисков; – план по обработке рисков; – частные политики безопасности.

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

– на оценку «**зачтено**» – обучающийся должен показать пороговый уровень знаний на уровне воспроизведения и объяснения информации;

– на оценку «**не зачтено**» – обучающийся 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), 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.

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):

a) предоставляемыми преподавателем на лекционных занятиях;

b) предоставляемыми преподавателем в рамках электронных образовательных курсов;

c) содержащимися в учебниках и учебных пособиях ЭБС (электронно-библиотечных систем), электронных каталогов университета и интернет-ресурсов.

2) Подробно разобрать типовые примеры решения задач, рассмотренные в рамках аудиторной контактной работы с преподавателем.

3) Применить полученные теоретические знания и практические навыки к решению индивидуальных заданий, к прохождению компьютерных тестирований.

4) При необходимости, сформировать перечень вопросов, вызвавших затруднения в процессе самостоятельной работы. Обсудить возникшие вопросы 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 пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.