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
_____ С.И. Лукьянов

26.02.2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Направление подготовки (специальность)
10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ
Направленность (профиль/специализация) программы
10.05.03 специализация N 7 "Обеспечение информационной безопасности распределенных информационных систем";

Уровень высшего образования - специалитет

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Информатики и информационной безопасности
Курс	5
Семестр	9

Магнитогорск
2020 год

Рабочая программа составлена на основе ФГОС ВО по специальности 10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ (приказ Минобрнауки России от 01.12.2016 г. № 1509)

Рабочая программа рассмотрена и одобрена на заседании кафедры Информатики и информационной безопасности
18.02.2020, протокол № 6

Зав. кафедрой _____ И.И. Баранкова

Рабочая программа одобрена методической комиссией ИЭиАС
26.02.2020 г. протокол № 5

Председатель _____ С.И. Лукьянов

Рабочая программа составлена:
доцент кафедры ИиИБ, канд. техн. наук _____ У.В. Михайлова

Рецензент:
Начальник отдела информационной безопасности АО "КУБ" .
_____ М.М. Близнецов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 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 2022 - 2023 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 2023 - 2024 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 2024 - 2025 учебном году на заседании кафедры Информатики и информационной безопасности

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

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Информатики и информационной безопасности

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

1 Цели освоения дисциплины (модуля)

Целями изучения дисциплины «Системы управления информационной безопасностью» являются: формирование компетенций по созданию части системы менеджмента предприятий/организаций предназначенной для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования информационной безопасности.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Системы управления информационной безопасностью входит в вариативную часть учебного плана образовательной программы.

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

Введение в специальность

Организация ЭВМ и вычислительных систем

Основы безопасности цифрового общества

Информатика

Языки программирования

Основы Data инжиниринга

Теория вероятностей, математическая статистика

Основы информационной безопасности

Учебная-практика по получению первичных профессиональных умений, в том числе первичных умений и навыков научно-исследовательской деятельности

Сети и системы передачи информации

Правоведение

Теория графов и ее приложения

Моделирование угроз информационной безопасности

Математическая логика и теория алгоритмов

Технологии и методы программирования

Технология построения защищенных распределенных приложений

Программно-аппаратные средства обеспечения информационной безопасности

Основы теории оптимизации

Математическое моделирование распределенных систем

Безопасность сетей ЭВМ

Безопасность Интернета вещей

Безопасность систем баз данных

Техническая защита информации

Тестирование систем защиты информации автоматизированных систем

Организационное и правовое обеспечение информационной безопасности

Разработка и эксплуатация защищенных автоматизированных систем

Разработка эксплуатационной документации на системы защиты информации автоматизированных систем

Безопасность операционных систем

Информационная безопасность распределенных информационных систем

Производственная-практика по получению профессиональных умений и опыта профессиональной деятельности

Методы и стандарты оценки защищенности компьютерных систем

Криптографические методы защиты информации

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

Подготовка к сдаче и сдача государственного экзамена

Производственная-преддипломная практика

Управление информационной безопасностью
Научно-исследовательская работа
Подготовка к защите и защита выпускной квалификационной работы

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

В результате освоения дисциплины (модуля) «Системы управления информационной безопасностью» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	
Знать	- нормативные методические документы ФСТЭК России в области ИБ АС; - основные угрозы безопасности информации и модели нарушителя в АС; - способы оптимизации систем управления информационной безопасности (СУИБ).
Уметь	- анализировать применяемые инструменты в области проектирования и управления ИБ с учетом стоимости и категорирования защищаемых объектов; - обосновывать целесообразность применяемых мер по обеспечению ИБ; - разрабатывать предложения по совершенствованию СУИБ АС.
Владеть	- навыками расследования инцидентов ИБ; - навыками сбора и анализа исходных данных, проведение обследования бизнес-процессов компании, входящих в область действия СУИБ; - навыками оценки активов (первичных и вторичных) компании, входящих в область действия СУИБ; - навыками определения владельцев и ценности активов;
ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	
Знать	- принципы разработки политики информационной безопасности компании/организации; - области действия СУИБ;
Уметь	- разрабатывать частные Политики ИБ; - определять цели и механизмы контроля обработки рисков ИБ и оценки их применимости для конкретного решения;
Владеть	- навыками обучение и повышение осведомленности персонала предприятия/организации в области обеспечения безопасности информации; - навыками документирование процессов управления ИБ (политики, процедуры, записи);
ПК-28 способностью управлять информационной безопасностью автоматизированной системы	

Знать	- отечественные и международные стандарты по информационной безопасности; - требования в области ИБ для создания, развития и поддержания системы менеджмента информационной безопасности (СМИБ)
Уметь	- разрабатывать техническое задание на проектирование СУИБ с учетом выявленных рисков ИБ - выбирать и анализировать технические решения для СУИБ;
Владеть	- навыками проведения предварительной оценки на предмет соответствия существующих механизмов управления и обеспечения ИБ в организации/компании требованиям международных стандартов; - навыками проведения предварительной оценки на предмет соответствия существующих механизмов управления и обеспечения ИБ в организации/компании требованиям стандартов и законодательства РФ;

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 2 зачетных единиц 72 акад. часов, в том числе:

– контактная работа – 37 акад. часов:

– аудиторная – 36 акад. часов;

– внеаудиторная – 1 акад. часов

– самостоятельная работа – 35 акад. часов;

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. Средства обеспечения безопасности корпоративной инфраструктуры								
1.1 Особенности корпоративной инфраструктуры	9	3	3		5	Подготовка к практическим занятиям. Самостоятельное изучение учебной и научной литературы, работа с материалами образовательног о портала и ЭБС	ИДЗ	ПК-19, ПК-22, ПК-28
1.2 Основные средства обеспечения безопасности корпоративной инфраструктуры: Системы обнаружения компьютерных атак. Системы мониторинга корпоративной инфраструктуры.		3	3		5	Подготовка к практическим занятиям. Самостоятельное изучение учебной и научной литературы, работа с материалами образовательног о портала и ЭБС	ИДЗ	ПК-19, ПК-22, ПК-28
Итого по разделу		6	6		10			
2. Кибербезопасность корпоративной инфраструткуры.								

2.1 Центры мониторинга инцидентов информационной безопасности. Системы мониторинга и управления ИБ (SIEM). Компоненты центра мониторинга. Системы взаимодействия между компонентами центра	9	3	3		5			ПК-19, ПК-22, ПК-28
2.2 Модели безопасности и передовая практика. Анатомия уязвимостей и бреши в данных. Проблемы безопасности с позиции модели STRIDE. Изучение методов, применяемых хакерами и инсайдерами. Способы проникновения в корпоративную сеть. Технические аспекты проникновения. Организация подключения к внутренним сервисам используя реверсивные		3	3		5			ПК-19, ПК-22, ПК-28
2.3 Рамки безопасности. Эшелонированная оборона и 4 периметра.		3	3		5			ПК-19, ПК-22, ПК-28
2.4 Особенности работы облачных приложений. Безопасность облачных приложений.		3	3		5			ПК-19, ПК-22, ПК-28
Итого по разделу		12	12		20			
3. Зачет								
3.1 Подготовка к зачету	9				5	Подготовка к зачету. Самостоятельное изучение учебной и научной литературы, работа с материалами образовательног о портала и ЭБС	Зачет	ПК-19, ПК-22, ПК-28
Итого по разделу					5			
Итого за семестр		18	18		35		зачёт	
Итого по дисциплине		18	18		35		зачет	ПК-19,ПК-22,ПК-28

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. Формы учебных занятий с использованием традиционных технологий:

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. Формы учебных занятий с использованием традиционных технологий:

a) Вводная лекция – для целостного представления об учебном предмете и анализа учебно-методической литературы;

b) Обзорные лекции – для систематизации научных знаний на высоком уровне с использованием ассоциативных связей в процессе представления и осмысления информации;

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

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

e) Практическое занятие, посвященное освоению конкретных умений и навыков по предложенному алгоритму;

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

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. Формы учебных занятий с использованием Раздельно-компетентностной технологии:

a) Кейс-методы – для овладения системой знаний и умений и творческого их использования в профессиональной деятельности и самообразовании; для квалифицированного и независимого решения профессиональных задач; для ориентации в многообразии учебных программ, пособий, литературы и выбора наиболее эффективных в применении к конкретной ситуации; для осуществления саморефлексии для дальнейшего профессионального, творческого роста и социализации личности.

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. Формы учебных занятий с использованием интерактивных технологий:

a) Case-study – для анализа реальных проблемных ситуаций и поиска лучших вариантов решений, разбор результатов тематических контрольных работ, анализ ошибок, совместный поиск вариантов рационального решения проблемы.

b) Методы IT – для применения компьютеров в процессе освоения дисциплины и доступа к ЭОР кафедры и Интернет-ресурсам.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Управление информационной безопасностью» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

Аудиторная самостоятельная работа обучающихся предполагает решение контрольных задач на практических занятиях.

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

Внеаудиторная самостоятельная работа обучающихся осуществляется в виде изучения литературы по соответствующему разделу с проработкой материала; выполнения домашних заданий, подготовки к аудиторным контрольным работам и выполнения домашних заданий с консультациями преподавателя.

Примерные задания:

Задание1: Провести анализ информационной инфраструктуры предприятия. Адаптировать базовую модель угроз для заданного случая.

Задание2: Разработать частную политику безопасности.

Задание3: Составить перечень организационных документов для СУИБ.

7 Оценочные средства для проведения промежуточной аттестации

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

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
ПК-19 способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы		
Знать	- нормативные методические документы ФСТЭК России в области ИБ АС; - основные угрозы безопасности информации и модели нарушителя в АС; - способы оптимизации систем управления информационной безопасности (СУИБ).	Теоретические вопросы: 1. Модель угроз информационной безопасности STRIDE 2. Модель оценки рисков DREAD 3. Нормативные и правовые акты, методические документы и национальные стандарты РФ в области обеспечения безопасности, относящиеся к управлению информационной безопасностью.
Уметь	- анализировать применяемые инструменты в области проектирования и управления ИБ с учетом стоимости и категорирования защищаемых объектов; - обосновывать целесообразность применяемых мер по обеспечению ИБ; - разрабатывать предложения по совершенствованию СУИБ АС.	Задания: 1. Выбрать решение для защиты выбранной корпоративной инфраструктуры. 2. Обосновать целесообразность выбранного решения для защиты выбранной корпоративной инфраструктуры.
Владеть	- навыками расследования инцидентов ИБ; - навыками сбора и анализа исходных данных, проведение обследования бизнес-процессов компании, входящих в область действия СУИБ; - навыками оценки активов (первичных и вторичных) компании, входящих в область действия СУИБ; - навыками определения владельцев и ценности активов;	Задания: 1. Определить основные векторы атак и попытаться смоделировать их на выбранной корпоративной инфраструктуре. 2. Провести анализ GPO средствами SCM. 3. Протестировать на проникновение инструментом OWASP ZAP выбранное веб-приложение.
ПК-22 способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации		

Структурный элемент компетенции	**Планируемые результаты обучения**	**Оценочные средства**
Знать	- принципы разработки политики информационной безопасности компании/организации; - области действия СУИБ;	Теоретические вопросы: 1. Основные принципы создания СУИБ 2. Эффективное управление политиками безопасности
Уметь	- разрабатывать частные Политики ИБ; - определять цели и механизмы контроля обработки рисков ИБ и оценки их применимости для конкретного решения;	Задания: 1. Подобрать оптимальную для выбранной корпоративной инфраструктуры СУИБ из имеющихся в данный момент на рынке предложений. Обосновать выбор. 2. Провести анализ конфигураций политик безопасности с целью обеспечения их согласованности для выбранной корпоративной инфраструктуры.
Владеть	- навыками обучение и повышение осведомленности персонала предприятия/организации в области обеспечения безопасности информации; - навыками документирование процессов управления ИБ (политики, процедуры, записи);	Задания: 1. Смоделировать шаблоны политик безопасности для выбранной корпоративной инфраструктуры с установленными продуктами безопасности Cisco для дальнейшего создания шаблонов политик безопасности.
ПК-28 способностью управлять информационной безопасностью автоматизированной системы		
Знать	- отечественные и международные стандарты по информационной безопасности; - требования в области ИБ для создания, развития и поддержания системы менеджмента информационной безопасности (СМИБ)	Теоретические вопросы: 1. Международный стандарт ISO/IEC 27001:2005 «Системы управления информационной безопасности. Требования» 2. Требования к аудиту ИБ. Международные стандарты. Нормативные документы РФ. Практика регуляторов. 3. Усиление защиты домена через групповые политики в соответствии с рекомендациями SCM.
Уметь	- разрабатывать техническое задание на проектирование СУИБ с учетом выявленных рисков ИБ - выбирать и анализировать технические решения для СУИБ;	Задания: 1. Выбрать и проанализировать необходимые компоненты для защиты корпоративной инфраструктуры (IDS/IPS, Firewall, AV, Monitoring) 2. Разработать ТЗ на проектирование СУИБ для выбранной корпоративной инфраструктуры.
Владеть	- навыками проведения предварительной оценки на предмет соответствия существующих механизмов управления и обеспечения ИБ в организации/компании требованиям международных стандартов; - навыками проведения предварительной оценки на предмет соответствия существующих механизмов управления и обеспечения ИБ в организации/компании требованиям стандартов и законодательства РФ;	Задания: 1. Проанализировать методики, документацию, инструменты и технологии в области безопасности веб – приложений на Project Application Security Open Web (OWASP). 2. Проанализировать существующие облачные платформы для использования в выбранной корпоративной инфраструктуре с учетом ее особенностей и требованиям обеспечения безопасности.

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

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

– на оценку **«не зачтено»** – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать навыки решения типовых задач.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. 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://new.znanium.com/catalog/product/997108 (дата обращения: 15.02.2020)

2.Внуков, А. А. Защита информации в банковских системах : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/414083 (дата обращения: 15.02.2020).

б) Дополнительная литература:

1. Баранкова И. И. Сетевая защита информации. Лабораторный практикум [Электронный ресурс] : учебное пособие [для вузов] / И. И., Баранкова, Д.Н. Мазнин, 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. - ISBN 978-5-9967-1605-0 URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3824.pdf&show=dcatalogues/1/1530260/3824.pdf&view=true (дата обращения 31.08.2020) - Макрообъект*

2. Душкин, А. В. Методологические основы построения защищенных автоматизированных систем: Монография / Душкин А.В. - Воронеж:Научная книга, 2016. - 76 с. ISBN 978-5-4446-0902-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/923295 (дата обращения: 15.02.2020)

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ

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

в) Методические указания:

1. Методические указания по выполнению лабораторных работ. (Приложение 1.)
2. Методические указания по выполнению внеаудиторных самостоятельных работ. (Приложение 2.)

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия
MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно

MS Office Visio Prof 2013(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2016(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2019(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
LibreOffice	свободно распространяемое ПО	бессрочно
Adobe Reader	свободно распространяемое ПО	бессрочно
MS Windows 10 Professional (для классов)	Д-1227-18 от 08.10.2018	11.10.2021
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Linux Calculate	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название ресурса	Ссылка
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Информационная система - Единое окно доступа к информационным ресурсам	URL: http://window.edu.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/
Российская Государственная библиотека. Каталоги	alogues/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	Default.asp
Университетская информационная система РОССИЯ	https://uisrussia.msu.ru
Международная наукометрическая реферативная и полнотекстовая база данных научных изданий «Web of science»	http://webofscience.com
Международная реферативная и полнотекстовая справочная база данных научных изданий «Scopus»	http://scopus.com
Международная база полнотекстовых журналов Springer Journals	http://link.springer.com/
Международная коллекция научных протоколов по различным отраслям знаний Springer Protocols	http://www.springerprotocols.com/

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/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii
Информационная система - Банк данных угроз безопасности информации ФСТЭК России	https://bdu.fstec.ru/

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.

ПРИЛОЖЕНИЕ 1

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ЛАБОРАТОРНЫХ РАБОТ

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

Лабораторное занятие – это занятие, проводимое под руководством преподавателя в учебной аудитории (компьютерном классе университета или учебной специализированной лаборатории университета), направленное на углубление научно-теоретических знаний и получение лабораторных навыков решения типовых и прикладных задач.

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

Основными задачами лабораторных занятий являются:

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

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

Структура лабораторного занятия включает следующие компоненты: вступительная часть; ответы на вопросы обучающихся; практическая часть; заключительное слово преподавателя. Во вступительной части объявляется тема текущей лабораторной работы, ставится ее цели и задачи, проводиться инструктаж по технике безопасности выполнения работы, проверяется исходный уровень готовности студентов к лабораторной работе (выполнение тестов, контрольные вопросы и т.п.), выдается порядок и условия выполнения лабораторной работы.

На лабораторном 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 лабораторных работ

Общие правила:

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

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

Лабораторная работа выполняется каждым студентом самостоятельно, согласно индивидуальному заданию.

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

После выполнения каждой лабораторной работы студент демонстрирует результат выполнения преподавателю в виде отчета по лабораторной работе и отвечает на вопросы.

Преподаватель оценивает работу в соответствии с заданными критериями оценки лабораторных работ.

Правила оформления результатов и оценивания лабораторной работы

Результаты выполненной лабораторной 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 прилагаются 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 2

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.