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)

ЗАЩИТА ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИХ РЕСУРСОВ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

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:
зав. кафедрой 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 2020 - 2021 учебном году на заседании кафедры Информатики и информационной безопасности

Протокол от 1 сентября 2020 г. № 1
Зав. кафедрой _____ И.И. Баранкова

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

1 Цели освоения дисциплины (модуля)

Целями изучения дисциплины «Защита информационно-технологических ресурсов автоматизированных систем» является формирование у обучающихся навыков определения информационно-технологических ресурсов автоматизированных систем подлежащих защите; проведения исследований информационно-технологических ресурсов; разработки частной модели угроз и нарушителя информационной безопасности; оценки соответствия защиты информационно-технологических ресурсов автоматизированных систем актуальных стандартам в области защиты информации; формирование рекомендаций по комплексу мер направленных на повышение эффективности существующей системы защиты информации в соответствии с требованиями ФГОС ВО по специальности 10.05.03 «Информационная безопасность автоматизированных систем».

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Защита информационно-технологических ресурсов автоматизированных систем входит в вариативную часть учебного плана образовательной программы.

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

Организация ЭВМ и вычислительных систем

Информатика

Сети и системы передачи информации

Моделирование угроз информационной безопасности

Программно-аппаратные средства обеспечения информационной безопасности

Безопасность систем баз данных

Безопасность сетей ЭВМ

Техническая защита информации

Тестирование систем защиты информации автоматизированных систем

Методы выявления нарушений информационной безопасности

Информационная безопасность распределенных информационных систем

Разработка и эксплуатация защищенных автоматизированных систем

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:

Производственная-преддипломная практика

Научно-исследовательская работа

Подготовка к сдаче и сдача государственного экзамена

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) «Защита информационно-технологических ресурсов автоматизированных систем» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ПК-2 способностью создавать и исследовать модели автоматизированных систем	

Знать	- структуру и состав автоматизированных систем управления - информационные и технологические ресурсы автоматизированных систем - способы определения и представления информационных потоков автоматизированных систем
Уметь	- проводить исследование модели автоматизированной системы - определять и классифицировать информационно-технологические ресурсы АС
Владеть	- навыками анализа информационной инфраструктуры автоматизированной системы; - навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите.
ПСК-7.1 способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	
Знать	- нормативные правовые акты, стандарты и руководящие документы в области защиты информации; - порядок разработки модели угроз - виды нарушителей информационной безопасности
Уметь	- определять подлежащие защите информационно-технологические ресурсы автоматизированных систем; - классифицировать и оценивать угрозы безопасности информации; - оценивать потенциал нарушителя информационной безопасности
Владеть	- методами выявления угроз безопасности информации в автоматизированных системах; - методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе.

4. Структура, объём и содержание дисциплины (модуля)

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

– контактная работа – 77,6 акад. часов:

– аудиторная – 72 акад. часов;

– внеаудиторная – 5,6 акад. часов

– самостоятельная работа – 30,7 акад. часов;

– подготовка к экзамену – 35,7 акад. часа

Форма аттестации - курсовой проект, экзамен

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. Аудит информационной безопасности информационно-технологических ресурсов автоматизированных систем								
1.1 Правовые и методологические основы аудита информационной безопасности.	9	2		2/2И	1	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	тестирование	ПК-2, ПСК-7.1

1.2 Виды аудита безопасности. Состав работ по проведению аудита безопасности		4		4/2И	1	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	тестирование	ПК-2, ПСК-7.1
Итого по разделу		6		6/4И	2			
2. Этапы проведения аудита информационной безопасности								
2.1 Постановка задач и уточнение состава работ	9	4		4/2И	1	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	тестирование. Практическая работа 1	ПК-2, ПСК-7.1
2.2 Сбор данных в соответствии с детальным перечнем работ, определенных в ТЗ на аудит		4		4/2И	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	тестирование. Практическая работа 2	ПК-2, ПСК-7.1

2.3 Анализ собранных данных, оценка рисков		6		6/4И	2	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	тестирование. Практическая работа 3	ПК-2, ПСК-7.1
2.4 Формирование рекомендаций по совершенствованию комплексной системы обеспечения информационной безопасности		6		6/4И	1	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	тестирование. Практическая работа 4	ПК-2, ПСК-7.1
2.5 Разработка плана мероприятий по устранению уязвимостей и недостатков в обеспечение информационной безопасности		6		6/6И	1	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	тестирование. Практическая работа 5	ПК-2, ПСК-7.1

2.6 Подготовка и оформление итогового отчета об аудите.		4		4	1,7	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка к тестированию; подготовка к практическому занятию	тестирование. Практическая работа 6	ПК-2, ПСК-7.1
Итого по разделу		30		30/18И	8,7			
3. Промежуточная аттестация								
3.1 Курсовой проект	9				20	Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями);подготовка курсового проекта	Защита курсового проекта	ПК-2, ПСК-7.1
3.2 Экзамен						Подготовка к практическому занятию; поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)	экзамен	ПК-2, ПСК-7.1
Итого по разделу					20			
Итого за семестр		36		36/22И	30,7		экзамен,кп	
Итого по дисциплине		36		36/22И	30,7		курсовой проект, экзамен	ПК-2,ПСК-7.1

5 Образовательные технологии

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Защита информационно-технологических ресурсов автоматизированных систем» 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

По дисциплине «Защита информационно-технологических ресурсов автоматизированных систем» предусмотрена аудиторная и внеаудиторная самостоятельная работа обучающихся.

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

Аудиторная самостоятельная работа обучающихся на практических занятиях осуществляется под контролем преподавателя в виде выполнения лабораторных работ, которые определяет преподаватель для обучающегося.

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 и вопросы по темам:

Перечень вопросов контрольных работ и тестирования по темам разделов 1-2:

1. Основные виды аудита безопасности
2. Опишите экспертный аудит
3. Опишите инструментальный анализ защищенности
4. Основные этапы работ при проведении аудита
5. Регламент проведения аудита
6. Сбор исходных данных для проведения аудита
7. Оценка текущего уровня безопасности
8. Классификация автоматизированных систем и требования по защите информации
9. Опишите что входит в состав организационно-распорядительная документации по вопросам информационной безопасности при сборе исходных данных
10. Опишите что входит в состав информации об аппаратном обеспечении хостов при сборе исходных данных
11. Опишите что входит в состав информации об общесистемном ПО при сборе исходных данных
12. Опишите что входит в состав информации о прикладном ПО при сборе исходных данных

13. Опишите что входит в состав информации о средствах защиты, установленных в АС при сборе исходных данных
14. Опишите что входит в состав информации о топологии АС при сборе исходных данных
15. Что необходимо указывать в описании границ, в рамках которых был проведён аудит безопасности при формировании отчета
16. Что необходимо указывать в описании структуры АС Заказчика при формировании отчета
17. Что необходимо указывать в описании методов и средств, которые использовались в процессе проведения аудита при формировании отчета
18. Что необходимо указывать в описании выявленных уязвимостей и недостатков при формировании отчета
19. Что необходимо указать в рекомендациях по совершенствованию комплексной системы обеспечения информационной безопасности при формировании отчета
20. Что необходимо указать в предложениях по плану реализации первоочередных мер, направленных на минимизацию выявленных рисков при формировании отчета

Пример практической работы 1. Постановка задач и уточнение состава работ

Сформировать ТЗ на аудит информационной безопасности информационно-технологических ресурсов автоматизированной системы, в которое входит:

1. Общие сведения
2. Цели и задачи проекта
3. Границы проведения работ
4. Требования к выполнению работ
5. Требования к Исполнителю
6. Этапы и сроки оказания услуг

Информационная система предприятия состоит из отдела кадров и бухгалтерии. В каждом отделе используются по четыре персональных компьютера, МФУ, сетевой коммутатор. Базы данных отделов хранятся на одном сервере. У персональных компьютеров и сервера имеется выход в интернет. На персональных компьютерах и сервере установлены актуальные версии операционных систем семейства Windows и актуальная антивирусная защита.

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-2 способностью создавать и исследовать модели автоматизированных систем		
Знать	- структуру и состав автоматизированных систем управления - информационные и технологические ресурсы автоматизированных систем - способы определения и представления информационных потоков автоматизированных систем	Перечень вопросов: 1. Функциональная часть автоматизированной информационной системы 2. Виды автоматизированных информационных систем 3. Программное и техническое обеспечение АИС 4. Методология структурного анализа и проектирования, интегрирующая процесс моделирования (SADT) 5. Методология и стандарт функционального моделирования(IDEF0) 6. Методология моделирования и стандарт документирования процессов, происходящих в систем(IDEF3) 7. Диаграммы потоков данных(DFD)
Уметь:	- проводить исследование модели автоматизированной системы - определять и классифицировать информационно-технологические ресурсы АС	Разработать диаграмму потоков данных для следующих АИС: 1. Охранная частная организация 2. Медицинское учреждение 3. Образовательное учреждение Определить и классифицировать информационно-технологические ресурсы
Владеть	- навыками анализа информационной инфраструктуры автоматизированной системы; - навыками определения информационной инфраструктуры и информационных ресурсов организации, подлежащих защите.	Разработать модели потоков данных и процессов, происходящих в системе, для следующих АИС: 1. Охранная частная организация 2. Медицинское учреждение 3. Образовательное учреждение Провести анализ информационной инфраструктуры. Определить и категорировать информационные ресурсы организации подлежащие защите.
ПСК-7.1 способностью разрабатывать и исследовать модели информационно- технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах		

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
Знать	- нормативные правовые акты, стандарты и руководящие документы в области защиты информации; - порядок разработки модели угроз - виды нарушителей информационной безопасности	Перечень вопросов: 1. Процесс определения угроз безопасности информации в информационной системе 2. Типы и виды нарушителей 3. Возможные цели и потенциал нарушителе 4. Оценка возможностей нарушителя по реализации угроз безопасности информации (разработка модели нарушителя) 5. Определение актуальных угроз безопасности информации в информационной системе 6. Показатель актуальности угрозы безопасности информации 7. Оценка вероятности (возможности) реализации угрозы безопасности информации 8. Показатели, характеризующие проектную защищенность информационной системы 9. Определение уровня проектной защищенности информационной системы 10. Ооценка степени возможного ущерба от реализации угрозы безопасности информации 11. Результат реализации угрозы безопасности информации 12. Основные виды ущерба и возможные негативные последствия 13. Формирование экспертной группы 14. Проведение экспертной оценки 15. Определение показателя «техническая компетентность нарушителя» 16. определение показателя «возможности нарушителя по доступу к информационной системе»
Уметь	- определять подлежащие защите информационно-технологические ресурсы автоматизированных систем; - классифицировать и оценивать угрозы безопасности информации; - оценивать потенциал нарушителя информационной безопасности	По представленным исходных данным об автоматизированной системе определить: 1. Подлежащие защите информационно-технологические ресурсы 2. Разработать модель угроз 3. Определить нарушителя, его потенциал. 4. Составить модель нарушителя
Владеть	- методами выявления угроз безопасности	По представленным исходных данным об автоматизированной системе определить: 1. Границы обследуемой автоматизированной

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	информации в автоматизированных системах; - методами оценки последствий от реализации угроз безопасности информации в автоматизированной системе.	информационной системы 2. Проектный уровень защищенности АС 3. Вероятность определяемых угроз 4. Актуальность угроз 5. Степень ущерба и последствия от реализации актуальных угроз

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

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме экзамена и курсового проекта.

Показатели и критерии оценивания экзамена:

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

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

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

– на оценку **«неудовлетворительно»** (2 балла) – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

– на оценку **«неудовлетворительно»** (1 балл) – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.

Показатели и критерии оценивания курсового проекта:

– на оценку **«отлично»** (5 баллов) – работа выполнена в соответствии с заданием, обучающийся показывает высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;

– на оценку **«хорошо»** (4 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения

уникальных ответов к проблемам;

– на оценку **«удовлетворительно»** (3 балла) – работа выполнена в соответствии с заданием, обучающийся показывает знания на уровне воспроизведения и объяснения информации, интеллектуальные навыки решения простых задач;

– на оценку **«неудовлетворительно»** (2 балла) – задание преподавателя выполнено частично, в процессе защиты работы обучающийся допускает существенные ошибки, не может показать интеллектуальные навыки решения поставленной задачи.

– на оценку **«неудовлетворительно»** (1 балл) – задание преподавателя выполнено частично, обучающийся не может воспроизвести и объяснить содержание, не может показать интеллектуальные навыки решения поставленной задачи.

Темы курсовых проектов:

По предоставленным исходным данным об объекте провести анализ, составить модель угроз и модель нарушителя. Сформировать рекомендации по совершенствованию комплексной системы обеспечения информационной безопасности. Разработать плана мероприятий по устранению уязвимостей и недостатков в обеспечение информационной безопасности. Исходные данные об объекте выдает преподаватель с зависимости от варианта исследуемой автоматизированной информационной системы.

Список организаций:

1. Отдел кадров предприятия
2. Система абитуриент учебного учреждения, подключенная к ГИС
3. Частная охранная организация с филиалами в разных городах.
4. Сегмент Единой Биометрической Системы
5. Частная коммерческая организация грузоперевозок
6. АСУ технологического участка производства
7. Клиентский отдел энергетической компании

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, 2020. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/422772 (дата обращения: 31.08.2020).

2. Зашита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва : РИОР: ИНФРА-М, 2019. - 400 с. - (Высшее образование). - DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-16-106478-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1018901 (дата обращения: 31.08.2020)

б) Дополнительная литература:

1. 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: 31.08.2020).

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: 31.08.2020)

МАКРООБЪЕКТЫ:

3. 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)

4. Баранков В. В. Развертывание и настройка виртуальных сетей [Электронный ресурс] : учебное пособие [для вузов] / В. В. Баранков, И. И. Баранкова, У. В. Михайлова, О. Б. Калугина] ; МГТУ. - Магнитогорск : МГТУ, 2019. - 1 электрон. опт. диск (CD-ROM). - ISBN 978-5-9967-1305-9 URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3813.pdf&show=dcatalogues/1/1529986/3813.pdf&view=true (дата обращения 31.08.2020)

5. Архитектура и принципы работы вычислительных систем [Электронный ресурс] : учебное пособие [для вузов] / В.В. Баранков, И.И. Баранкова, М.В. Афанасьева, М.В. Коновалов; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - ISBN 978-5-9967-1306-6 URL : https://magtu.informsystema.ru/uploader/fileUpload?name=3924.pdf&show=dcatalogues/1/1530495/3924.pdf&view=true (дата обращения 31.08.2020)

6. Баранкова, И. И. Михайлова У.В. , Лукьянов Г.И. Техническая защита информации. Лабораторный практикум [Электронный ресурс] : учебное пособие / МГТУ. - Магнитогорск : МГТУ, 2017. - 1 электрон. опт. диск (CD-ROM). URL : https://magtu.informsystema.ru/uploader/fileUpload?name=2935.pdf&show=dcatalogues/1/1134667/2935.pdf&view=true (дата обращения 31.08.2020)

*РЕЖИМ ПРОСМОТРА МАКРООБЪЕКТОВ
1. Перейти по адресу электронного каталога https://magtu.informsystema.ru
2. Произвести авторизацию (Логин: Читатель1 Пароль: 111111)
3. Активизировать гиперссылку макрообъекта
*При открытии макрообъектов учитывайте настройки антивирусной защиты

в) Методические указания:

1. Методические указания по выполнению практических работ по дисциплине «Защита информационно-технологических ресурсов автоматизированных систем» (Приложение 1) .

2. Методические указания по выполнению внеаудиторных самостоятельных работ по дисциплине «Защита информационно-технологических ресурсов автоматизированных систем» (Приложение 2).

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
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
Oracle Virtual Box	свободно распространяемое ПО	бессрочно
MS Office Visio Prof 2007(для классов)	Д-1227-18 от 08.10.2018	11.10.2021

MS Office Visio Prof 2010(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
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
MS Office Visio Prof 2003(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Visio Prof 2002(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Access Prof 2003(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Access Prof 2007(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Access Prof 2010(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Access Prof 2013(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Office Access Prof 2016(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS SQL Server Management Studio	свободно распространяемое ПО	бессрочно
LibreOffice	свободно распространяемое ПО	бессрочно
MS Visual Studio 2013 Professional(для класса)	Д-1227-18 от 08.10.2018	11.10.2021
MS Visual Studio Code	свободно распространяемое ПО	бессрочно
MS Visual Studio 2017 Community Edition	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

MS Windows Server(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно	бессрочно
MariaDB	свободно	бессрочно
PostgreSQL	свободно	бессрочно
MS Office 2003 Professional	№ 135 от 17.09.2007	бессрочно
MS Windows XP Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
MS Visual Studio 2010 Professional(для класса)	Д-1227-18 от 08.10.2018	11.10.2021
FAR Manager	свободно	бессрочно
Linux Calculate	свободно	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Электронная база периодических изданий East View Information Services, ООО «ИВИС»	https://dlib.eastview.com/
Национальная информационно-аналитическая система – Российский индекс научного цитирования	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	https://www.rsl.ru/ru/4readers/catalogues/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	http://magtu.ru:8085/marcweb2/Default.asp
Федеральный образовательный портал – Экономика. Социология. Менеджмент	http://ecsocman.hse.ru/
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	http://scopus.com
Международная база полнотекстовых журналов Springer Journals	http://link.springer.com/
Международная коллекция научных протоколов по различным отраслям знаний	http://www.springerprotocols.com/

Международная база научных материалов в области	http://materials.springer.com/
Международная база справочных изданий по всем	http://www.springer.com/references
Международная реферативная база данных по чистой и	http://zbmath.org/
Международная реферативная и полнотекстовая справочная база данных научных изданий	https://www.nature.com/siteindex
Архив научных журналов «Национальный электронно-информационный	https://archive.neicon.ru/xmlui/
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:

Лекционная аудитория (ауд. 2124, ауд. 226, ауд. 365, ауд. 388 и т.д.)- Мультимедийные средства хранения, передачи и представления информации

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.

Аудитория для самостоятельной работы читальные залы библиотеки, ауд 132а - Персональные компьютеры с ПО и выходом в Интернет и доступом в электронную информационно-образовательную среду университета.

ПРИЛОЖЕНИЕ 1

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ ПРАКТИЧЕСКИХ РАБОТ

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

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

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

Основными задачами практических занятий являются:

- углубление уровня освоения общекультурных и профессиональных компетенций;
- обобщение, систематизация, углубление, закрепление полученных практических знаний по конкретным темам дисциплин различных циклов;
- приобретение обучающимися 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 обучающихся 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 обучающиеся 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 обучающийся должен повторить теоретический материал, необходимый для выполнения заданий по текущей теме.

Практическая работа выполняется каждым обучающимся самостоятельно, согласно индивидуальному заданию.

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

После выполнения каждой практической работы обучающийся 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 обучающийся 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 обучающийся 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 обучающихся 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 с обучающимися 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.