



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)**

***ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ***

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	1
Семестр	1

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. Блинецов

## 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)**

Целью дисциплины «Введение в специальность» является ознакомление обучающихся с профессиональной деятельностью в сфере разработки, исследования и эксплуатации систем обеспечения информационной безопасности автоматизированных систем в соответствии с требованиями ФГОС ВО для специальности 10.05.03 «Информационная безопасность автоматизированных систем». Дисциплина «Введение в специальность» содействует формированию мировоззрения и системного мышления, ориентирует обучающихся в широкой сфере проблем обеспечения информационной безопасности автоматизированных систем.

### **2 Место дисциплины (модуля) в структуре образовательной программы**

Дисциплина Введение в специальность входит в базовую часть учебного плана образовательной программы.

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

Дисциплина «Введение в специальность» входит в базовую часть блока 1 образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения «Информатика и информационно-коммуникационные технологии», «Алгебра» и «Физика» в объеме средней общеобразовательной школы.

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

Основы безопасности цифрового общества

Основы информационной безопасности

Моделирование угроз информационной безопасности

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

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

В результате освоения дисциплины (модуля) «Введение в специальность» обучающийся должен обладать следующими компетенциями:

Структурный элемент компетенции	Планируемые результаты обучения
ОК-5	способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
Знать	<ul style="list-style-type: none"><li>• политику государства в области обеспечения информационной безопасности</li><li>• национальные, межгосударственные и международные стандарты в области защиты информации</li><li>• современное состояние рынка труда в области обеспечения информационной безопасности</li><li>• профессиональный стандарт «Специалист по защите информации в автоматизированных системах»</li><li>• трудовое законодательство РФ</li></ul>

Уметь	<ul style="list-style-type: none"> <li>• анализировать информацию по вопросам национальной и информационной безопасности государства;</li> <li>• соблюдать нормы профессиональной этики</li> </ul>
Владеть	<ul style="list-style-type: none"> <li>• профессиональной терминологией в области информационной безопасности;</li> <li>• практическими навыками соблюдения норм профессиональной этики.</li> </ul>
ПК-1 способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	
Знать	<ul style="list-style-type: none"> <li>• Основы построения систем обработки и передачи информации, их современное состояние развития.</li> <li>• Основные задачи обеспечения безопасности информации в компьютерных и автоматизированных системах.</li> <li>• Особенности обработки информации с использованием компьютерных систем</li> </ul>
Уметь	<ul style="list-style-type: none"> <li>• Осуществлять поиск и систематизировать современную научно-техническую информацию по рассматриваемым вопросам в рамках дисциплины.</li> <li>• Анализировать современную научно-техническую информацию по рассматриваемым в рамках дисциплины проблемам и задачам.</li> </ul>
Владеть	<ul style="list-style-type: none"> <li>• Навыками сбора современной научно-технической информации по рассматриваемым в рамках дисциплины проблемам и задачам.</li> <li>• Навыками осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке</li> </ul>

#### 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. Доктрина информационной безопасности								
1.1 Общие положения. Основные информационные угрозы и состояние информационной безопасности.	1	1		1/ИИ	1	<p>Подготовка к семинарским, практическим занятиям</p> <p>Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями)</p> <p>Контрольная работа</p> <p>Разработка глоссария к теме</p> <p>Работа с электронными библиотеками</p>	<p>– устный опрос (собеседование);</p> <p>– контрольные работы;</p> <p>– коллоквиумы;</p> <p>– семинарские занятия;</p>	ОК-5, ПК-1

1.2 Стратегические цели и основные направления обеспечения информационной безопасности		1		1/ИИ	2	Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы; – коллоквиумы; – семинарские занятия;	ОК-5, ПК-1
Итого по разделу		2		2/ИИ	3			
2. Организационная основа системы обеспечения информационной безопасности								
2.1 Деятельность государственных органов по обеспечению информационной безопасности. Задачи государственных органов в рамках деятельности по обеспечению информационной безопасности. Задачи государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности	1	2		2/ИИ	4	Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы; – коллоквиумы; – семинарские занятия;	ОК-5, ПК-1
Итого по разделу		2		2/ИИ	4			
3. Национальные интересы РФ в информационной сфере								

<p>3.1 Обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации. Обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры</p>	1		1	2	<p>Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками</p>	<p>– устный опрос (собеседование); – контрольные работы; – коллоквиумы; – семинарские занятия;</p>	ОК-5, ПК-1
<p>3.2 Развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, в области обеспечения информационной безопасности. Содействие формированию системы международной информационной безопасности</p>	1		1	2	<p>Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками</p>	<p>– устный опрос (собеседование); – контрольные работы; – коллоквиумы; – семинарские занятия;</p>	ОК-5, ПК-1
Итого по разделу	2		2	4			
4. Способы нарушения информационной безопасности							



<p>4.1 Информационные, программно-аппаратные, физические, радиоэлектронные и организационно-правовые способы нарушения информационной безопасности</p>	1	2		2/ИИ	4	<p>Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками</p>	<p>– устный опрос (собеседование); – контрольные работы; – коллоквиумы; – семинарские занятия;</p>	ОК-5, ПК-1
<p>4.2 Результатами реализации угроз информационной безопасности и осуществления посягательств (способов воздействия) на информационные ресурсы, информационные системы, информационные процессы</p>	1	2		2/ИИ	4	<p>Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками</p>	<p>– устный опрос (собеседование); – контрольные работы; – коллоквиумы; – семинарские занятия;</p>	ОК-5, ПК-1
Итого по разделу		4		4/ИИ	8			
5. Информационные войны								

5.1 Классификация и способы информационной войны. Объекты воздействия. Источники угроз. Анализ риска информационной войны	1	2		2/ИИ	4	Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы; – коллоквиумы; – семинарские занятия;	ОК-5, ПК-1
Итого по разделу		2		2/ИИ	4			
6. Криптография и стеганография								
6.1 Классическая, компьютерная и цифровая стеганография. Атаки на стегосистемы. Применение стеганографии	1	1		1	2	Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы; – коллоквиумы; – семинарские занятия;	ОК-5, ПК-1

<p>6.2 Криптография и криптоанализ. Криптографические методы. Основные проблемы криптографии. Законодательство в области криптографии и стеганографии.</p>		1		1	2	<p>Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками</p>	<p>– устный опрос (собеседование); – контрольные работы; – коллоквиумы; – семинарские занятия;</p>	ОК-5, ПК-1
Итого по разделу		2		2	4			
7. Технические каналы утечки информации								
<p>7.1 Причины утечек данных и возможные ситуации. Классификация технических каналов утечки информации. Использование технических каналов утечки информации.</p>	1	2		2	4	<p>Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками</p>	<p>– устный опрос (собеседование); – контрольные работы; – коллоквиумы; – семинарские занятия;</p>	ОК-5, ПК-1

7.2 Средства и системы для обнаружения утечки информации. Способы защиты информации		2		2	4	Подготовка к семинарским, практическим занятиям Поиск дополнительной информации по заданной теме (работа с библиографическим материалами, справочниками, каталогами, словарями, энциклопедиями) Контрольная работа Разработка глоссария к теме Работа с электронными библиотеками	– устный опрос (собеседование); – контрольные работы; – коллоквиумы; – семинарские занятия;	ОК-5, ПК-1
Итого по разделу		4		4	8			
Итого за семестр		18		18/6И	35		зачёт	
Итого по дисциплине		18		18/6И	35		зачет	ОК-5, ПК-1

## **5 Образовательные технологии**

Для реализации предусмотренных видов учебной работы в качестве образовательных технологий в преподавании дисциплины «Введение в специальность» 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 «Введение в специальность» 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 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.

### **Темы рефератов**

1. Правовая охрана программ и данных. Защита информации.
2. Методы защиты информации
3. Системы защиты информации
4. Защита баз данных
5. Защита информации от несанкционированного доступа методом криптопреобразования
6. Защита цифровой информации методами стеганографии
7. Компьютерные вирусы, типы вирусов, методы борьбы с вирусами.
8. Информационный потенциал общества.
9. Человек в информационном обществе.
10. Коллективное использование разнородных информационных ресурсов

### **Перечень тем контрольных работ**

1. Концепция доктрины информационной безопасности РФ
2. Деятельность государственных органов по обеспечению информационной безопасности.
3. Национальные интересы РФ в информационной сфере
4. Информационные, программно-аппаратные, физические, радиоэлектронные и организационно-правовые способы нарушения информационной безопасности
5. Информационные войны
6. Криптография
7. Стеганография
8. Технические каналы утечки информации

9. Средства и системы для обнаружения утечки информации. Способы защиты информации

**Вопросы для зачета**

1. Понятие информационной безопасности государства.
2. Понятие целостности и конфиденциальности информации.
3. Требования защиты информации.
4. Общие положения, технические и организационные требования, составляющие
5. Доктрина информационной безопасности РФ.
6. Информационные войны. Классификация и способы информационной войны.
7. Классификация технических каналов утечки информации
8. Способы защиты информации от утечки по техническим каналам

**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
<p>ОК-5 - способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики</p>		
<p>Знать</p>	<ul style="list-style-type: none"> <li>• политику государства в области обеспечения информационной безопасности</li> <li>• национальные, межгосударственные и международные стандарты в области защиты информации</li> <li>• современное состояние рынка труда в области обеспечения информационной безопасности</li> <li>• профессиональный стандарт «Специалист по защите информации в автоматизированных системах»</li> <li>• трудовое законодательство РФ</li> </ul>	<p>Перечень вопросов:</p> <ol style="list-style-type: none"> <li>1. Понятие информационной безопасности государства.</li> <li>2. Понятие целостности и конфиденциальности информации.</li> <li>3. Требования защиты информации.</li> <li>4. Национальные интересы РФ в информационной сфере</li> <li>5. Общие положения доктрины информационной безопасности</li> <li>6. Классификация и способы информационной войны</li> </ol>
<p>Уметь</p>	<ul style="list-style-type: none"> <li>• анализировать информацию по вопросам национальной и информационной безопасности государства;</li> <li>• соблюдать нормы профессиональной этики</li> </ul>	<ol style="list-style-type: none"> <li>1. Проведите анализ доктрины информационной безопасности РФ и выделите основные направления обеспечения информационной безопасности в области обороны страны в соответствии с военной политикой Российской Федерации.</li> <li>2. Проведите анализ доктрины информационной безопасности РФ и выделите основные направления обеспечения информационной безопасности в области государственной и общественной безопасности.</li> </ol>

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		<p>3. Проведите анализ доктрины информационной безопасности РФ и выделите основные направления обеспечения информационной безопасности в экономической сфере</p> <p>4. Проведите анализ доктрины информационной безопасности РФ и выделите основные направления обеспечения информационной безопасности в области науки, технологий и образования</p> <p>5. Проведите анализ доктрины информационной безопасности РФ и выделите основные направления обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства</p>
Владеть	<ul style="list-style-type: none"> <li>• профессиональной терминологией в области информационной безопасности;</li> <li>• практическими навыками соблюдения норм профессиональной этики</li> </ul>	<ul style="list-style-type: none"> <li>• Разработать глоссарий по доктрине информационной безопасности РФ</li> <li>• Разработать глоссарий на тему информационные войны</li> </ul>
ПК-1 - способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке		
Знать	<ul style="list-style-type: none"> <li>• Основы построения систем обработки и передачи информации, их современное состояние развития.</li> <li>• Основные задачи обеспечения безопасности информации в компьютерных и автоматизированных системах.</li> <li>• Особенности обработки информации с использованием компьютерных систем</li> </ul>	<ol style="list-style-type: none"> <li>1. Дайте определение понятию «информация». Дайте определение понятию «информационные технологии».</li> <li>2. Дайте определение понятию «информационная система».</li> <li>3. Дайте определение понятию «информационно-телекоммуникационная сеть». Дайте определение понятию «обладатель информации». Назовите его права и обязанности</li> <li>4. Определите понятия «доступ к информации» и «конфиденциальность информации».</li> <li>5. Определите понятия «предоставление информации» и «распространение информации».</li> <li>6. Определите понятия «электронное сообщение», «документированная информация» и «электронный документ».</li> <li>7. Дайте определение понятию «оператор информационной системы»</li> <li>8. Определите классификацию информационных войн.</li> <li>9. Какие объекты воздействия у информационных войн?. Какие существуют технические каналы утечки информации?</li> <li>10. Как существуют средства защиты от</li> </ol>

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		утечки по техническим каналам? 11. Дайте определение стеганографии и криптографии. В чем их отличие?
Уметь	<ul style="list-style-type: none"> <li>• Осуществлять поиск и систематизировать современную научно-техническую информацию по рассматриваемым вопросам в рамках дисциплины.</li> <li>• Анализировать современную научно-техническую информацию по рассматриваемым в рамках дисциплины проблемам и задачам.</li> </ul>	<p>Провести анализ современной научно-технической информации на следующие темы:</p> <ol style="list-style-type: none"> <li>1. Правовая охрана программ и данных. Защита информации.</li> <li>2. Методы защиты информации</li> <li>3. Системы защиты информации</li> <li>4. Защита баз данных</li> <li>5. Защита информации от несанкционированного доступа методом криптопреобразования</li> <li>6. Защита цифровой информации методами стеганографии</li> <li>7. Компьютерные вирусы, типы вирусов, методы борьбы с вирусами.</li> <li>8. Информационный потенциал общества.</li> <li>9. Человек в информационном обществе.</li> <li>10. Коллективное использование разнородных информационных ресурсов</li> </ol>
Владеть	<ul style="list-style-type: none"> <li>• Навыками сбора современной научно-технической информации по рассматриваемым в рамках дисциплины проблемам и задачам.</li> <li>• Навыками осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке</li> </ul>	<ol style="list-style-type: none"> <li>1. Провести сравнительный анализ доктрины информационной безопасности от 2000г и 2016г</li> <li>2. Осуществить поиск и составить список основных федеральных законов в области информационной безопасности РФ</li> </ol>

**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.



## **8 Учебно-методическое и информационное обеспечение дисциплины (модуля)**

### **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/42277> 2 (дата обращения: 31.08.2020).

2. Защита 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. Ковалев, Д. В. Информационная безопасность: Учебное пособие / Ковалев Д.В., Богданова Е.А. - Ростов-на-Дону:Южный федеральный университет, 2016. - 74 с.: ISBN 978-5-9275-2364-1. - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/997105> (дата обращения: 31.08.2020)

2. Веселов, Г. Е. Менеджмент риска информационной безопасности: Учебное пособие / Веселов Г.Е., Абрамов Е.С., Шилов А.К. - Таганрог:Южный федеральный университет, 2016. - 107 с.: ISBN 978-5-9275-2327-5. - Текст : электронный. - URL: <https://new.znanium.com/catalog/product/997108> (дата обращения: 31.08.2020)

3. 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).

#### **МАКРООБЪЕКТЫ:**

4. 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)

**\*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 практических работ по дисциплине «Введение в специальность» (Приложение 1) .

2. Методические указания по выполнению внеаудиторных самостоятельных работ по дисциплине «Введение в специальность» (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	бессрочно
LibreOffice	свободно	бессрочно
Adobe Reader	свободно	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	бессрочно
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»	<a href="https://dlib.eastview.com/">https://dlib.eastview.com/</a>
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: <a href="https://elibrary.ru/project_risc.asp">https://elibrary.ru/project_risc.asp</a>
Поисковая система Академия Google (Google Scholar)	URL: <a href="https://scholar.google.ru/">https://scholar.google.ru/</a>
Информационная система - Единое окно доступа к информационным ресурсам	URL: <a href="http://window.edu.ru/">http://window.edu.ru/</a>
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: <a href="http://www1.fips.ru/">http://www1.fips.ru/</a>
Российская Государственная библиотека. КATALOGI	<a href="https://www.rsl.ru/ru/4readers/catalogues/">https://www.rsl.ru/ru/4readers/catalogues/</a>

Электронные ресурсы библиотеки МГТУ им. Г.И.	<a href="http://magtu.ru:8085/marcweb2/Default.asp">http://magtu.ru:8085/marcweb2/Default.asp</a>
Федеральный образовательный портал –	<a href="http://ecsocman.hse.ru/">http://ecsocman.hse.ru/</a>
Университетская информационная система	<a href="https://uisrussia.msu.ru">https://uisrussia.msu.ru</a>
Международная наукометрическая реферативная и	<a href="http://webofscience.com">http://webofscience.com</a>
Международная реферативная и полнотекстовая справочная	<a href="http://scopus.com">http://scopus.com</a>
Международная база полнотекстовых журналов	<a href="http://link.springer.com/">http://link.springer.com/</a>
Международная коллекция научных протоколов по	<a href="http://www.springerprotocols.com/">http://www.springerprotocols.com/</a>
Международная база научных материалов в области	<a href="http://materials.springer.com/">http://materials.springer.com/</a>
Международная база справочных изданий по всем	<a href="http://www.springer.com/references">http://www.springer.com/references</a>
Международная реферативная база данных по чистой и	<a href="http://zbmath.org/">http://zbmath.org/</a>
Международная реферативная и полнотекстовая справочная база данных научных изданий	<a href="https://www.nature.com/siteindex">https://www.nature.com/siteindex</a>
Архив научных журналов «Национальный электронно-информационный	<a href="https://archive.neicon.ru/xmlui/">https://archive.neicon.ru/xmlui/</a>
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические	<a href="https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-i-nformatsii">https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-i-nformatsii</a>
Информационная система - Банк данных угроз	<a href="https://bdu.fstec.ru/">https://bdu.fstec.ru/</a>

### **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.

## 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 ИТ, 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.

**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, аудиторские контрольные работы, компьютерное тестирование.

Максимальное количество баллов обучающийся получает, если:

- выполняет индивидуальные задания в соответствии со всеми заявленными требованиями;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать рациональность решения текущей задачи.;
- обстоятельно с достаточной полнотой излагает соответствующую теоретический раздел;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

50~85% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 70% от полного), но правильно выполнено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- дает правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания им данного материала.

36~50% от максимального количества баллов обучающийся получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, но допускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.

35% и менее от максимального количества баллов обучающийся получает, если:

- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки. В "0" баллов преподаватель вправе оценить выполненное обучающимся задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы или не было представлено для проверки.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель обучающегося. Рейтинговый показатель обучающегося влияет на выставление итоговой оценки по результатам изучения дисциплины.

Показатели и критерии оценивания полученных знаний представлены в пункте 7.б) «Оценочные средства для проведения промежуточной аттестации» данной РПД.