

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
**БАШКИРСКИЙ ИНСТИТУТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ (ФИЛИАЛ)**  
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО  
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ  
**«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ ИМЕНИ К.Г. РАЗУМОВСКОГО  
(ПЕРВЫЙ КАЗАЧИЙ УНИВЕРСИТЕТ)»**

**УТВЕРЖДАЮ**

Директор Башкирского института  
технологий и управления (филиал)

  
Е. В. Кузнецова

«29» июня 2023 г.



**Рабочая программа дисциплины (модуля)**

**Б1.В.ДВ.06.01 Аппаратные средства защиты технической  
информации на предприятиях пищевой промышленности**

Кафедра:	Информационные технологии и системы управления
Направление подготовки:	15.03.04 Автоматизация технологических процессов и производств
Направленность (профиль):	Автоматизация технологических процессов и производств в пищевой промышленности и отраслях агропромышленного комплекса
Тип образовательной программы:	Бакалавриат
Квалификация выпускника:	Бакалавр
Форма обучения:	Очно-заочная, заочная
Год набора:	2021
Общая трудоемкость:	144/4 з.е.

Мелеуз 2023

Программу составил:  
канд.пед.наук Яшин Д.Д.

Рабочая программа дисциплины (модуля) «Аппаратные средства защиты технической информации на предприятиях пищевой промышленности» разработана и составлена на основании учебного плана, утвержденного ученым советом в соответствии с ФГОС ВО Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств (уровень бакалавриата) (приказ Минобрнауки России от 12.03.2015 г. № 200)

Руководитель ОПОП  
канд.пед.наук Е. В. Одиноква



Рабочая программа согласована на заседании выпускающей кафедры  
«Информационные технологии и системы управления»  
Протокол от «29» июня 2023 года № 11

И.о. зав. кафедрой Е. В. Одиноква



## СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ) .....	4
2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ И ОБЪЕМ С РАСПРЕДЕЛЕНИЕМ ПО СЕМЕСТРАМ .....	4
3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ.....	5
4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ) .....	6
5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ.....	10
6. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ .....	11
7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ).....	16
8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ).....	16
9. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ .....	16

## 1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

### 1.1. Цели:

формирование компетентности в области разработки и эксплуатации автоматизированных систем в защищенном исполнении. отдельных компонентов автоматизированных систем управления, с учетом требований нормативно - технической и методической документации по обеспечению безопасности информации.

### 1.2. Задачи:

- изучение основных угроз безопасности информации в автоматизированных системах и освоение аппаратных методов защиты от данных угроз;
- изучение методов, алгоритмов, аппаратных средств обеспечения информационной безопасности автоматизированных систем;
- изучение современных технологий защищенных сетей передачи данных в автоматизированных системах.

## 2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ И ОБЪЕМ С РАСПРЕДЕЛЕНИЕМ ПО СЕМЕСТРАМ

Цикл (раздел) Б1.В.ДВ.06

Дисциплина относится к вариативной части ОПОП к дисциплине по выбору.

### Связь с предшествующими дисциплинами (модулями), практиками

№	Наименование дисциплины	Семестр	Шифр компетенции
1	Автоматизированный документооборот организации	6	ПК-33
2	Инструментальные средства разработки и оформления документов	6	ПК-33
3	Практика по получению профессиональных умений и опыта профессиональной деятельности	6	ОПК-1; ОПК-2; ОПК-5; ПК-7; ПК-8; ПК-10; ПК-29; ПК-30; ПК-31; ПК-32; ПК-33

### Связь с последующими дисциплинами (модулями), практиками

№	Наименование дисциплины	Семестр	Шифр компетенции
1	Преддипломная практика	8	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ОПК-5, ПК-7, ПК-8, ПК-9, ПК-10, ПК-11, ПК-29, ПК-30, ПК-31, ПК-32, ПК-33, ПК-18, ПК-19, ПК-20, ПК-21, ПК-22
2	Проектирование автоматизированных систем в пищевой промышленности и отраслях агропромышленного комплекса	8, 9	ПК-7; ПК-8; ПК-9; ПК-32; ПК-33

### Распределение часов дисциплины

#### Очно-заочная форма обучения

Семестр (Курс/Семестр на курсе)	7(4/1)		Итого	
	18 1/6			
Неделя	УП	РП	УП	РП
Вид занятий				
Лекции	8	8	8	8
Практические				
Лабораторные	8	8	8	8
Итого ауд.	16	16	16	16
Контактная работа	16	16	16	16
Сам. работа	128	128	128	128
Часы на контроль				
Итого	144	144	144	144

Вид промежуточной аттестации:

Зачет с оценкой 7 семестр

#### Заочная форма обучения

Семестр (Курс/Семестр на курсе)	7(4/1)		Итого	
	2 5/6			
Неделя	УП	РП	УП	РП
Вид занятий				
Лекции	2	2	2	2

Практические	4	4	4	4
Лабораторные	4	4	4	4
Итого ауд.	10	10	10	10
Контактная работа	10	10	10	10
Сам. работа	130	130	130	130
Часы на контроль	4	4	4	4
Итого	144	144	144	144

**Вид промежуточной аттестации:**

Зачет с оценкой 7 семестр

**3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

В результате изучения дисциплины «Аппаратные средства защиты технической информации на предприятиях пищевой промышленности» студент должен:

**знать:**

- виды, функции и требования к современным средствам аппаратной аутентификации пользователей в клиент-серверных приложениях;
- методы и аппаратные средства защиты программного обеспечения от несанкционированного изучения, копирования и модификации;
- методы и алгоритмы управления и генерации ключей и их аппаратно-программная реализация и применение в автоматизированных системах;
- принципы построения безопасных автоматизированных рабочих мест и вычислительных сетей с использованием аппаратных комплексов.

**уметь:**

- разворачивать и настраивать аппаратные средства для защиты локальных и распределенных вычислительных систем;
- обеспечивать надежную аутентификацию и управление доступом к информационным ресурсам с учетом требований нормативно-технической документации;
- настраивать каналы безопасного обмена информацией в локальных и распределенных автоматизированных системах.

**владеть:**

- инструментарием, обеспечивающим аппаратную защиту информационных ресурсов от изучения, модификации и копирования;
- аппаратными комплексами управления ключами, сертификатами и правами пользователей в защищенных автоматизированных системах.

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций:

**ПК-33 способностью участвовать в разработке новых автоматизированных и автоматических технологий производства продукции и их внедрении, оценке полученных результатов, подготовке технической документации по автоматизации производства и средств его оснащения**

#### 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

##### Очно-заочная форма обучения

Код занятия	Наименования разделов, тем, их краткое содержание и результаты освоения /вид занятия/	Семестр	Часов	Интеракт.	Прак. подг.	Формируемый признак компетенции	Оценочные средства
	<b>Раздел 1. Информационная безопасность и уровни ее обеспечения</b>						
1.1	Тема 1. Понятие «Информационная безопасность» Краткое содержание: Информационная безопасность. Защита информации. Основные составляющие информационной безопасности. Доступность, целостность и конфиденциальность информационных ресурсов. Важность и сложность проблемы информационной безопасности. Доктрина информационной безопасности Российской Федерации <b>знать:</b> современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования. <b>уметь:</b> выбрать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты <b>владеть:</b> методами защиты информации и программного обеспечения от несанкционированного доступа и копирования /лек/	7	2	0	0	ПК-33	Конспект
1.2	Тема 1. Составляющие информационной безопасности Краткое содержание: Основные составляющие. Важность проблемы. Понятие информационной безопасности. Защита информации. Основные составляющие информационной безопасности. Основные определения и критерии классификации угроз. Основные угрозы конфиденциальности. /лаб/	7	2	0	0	ПК-33	Отчет по лаб. работам
1.3	Тема 1. Информационная безопасность и уровни ее обеспечения Краткое содержание: изучить современную ситуацию в области информационной безопасности; категории информационной безопасности; абстрактные модели защиты информации, обзор наиболее распространенных методов "взлома" /ср/	7	40	0	0	ПК-33	Устный опрос
	<b>Раздел 2. Стандарты информационной безопасности</b>						
2.1	Тема 2. Стандарты информационной безопасности: "Общие критерии" Краткое содержание: Понятие безопасности информации. Международный стандарт информационной безопасности. Особенности процесса стандартизации в Интернете. Стандарты безопасности в Интернете: SSL (TLS), SET, IPSec. Особенности российского рынка. Государственные стандарты <b>знать:</b> устройство сетевых компонентов: сервера, рабочие станции, среда передачи информации и узлы коммутации сетей <b>уметь:</b> проектировать локальную сеть, объединяя сервера, рабочие станции и среду передачи информации	7	4	0	0	ПК-33	Конспект

	<b>владеть:</b> навыками монтажа локальной сети. /лек/						
2.2	Тема 2. Стандарты информационной безопасности распределенных систем Краткое содержание: Информационная безопасность распределенных систем. Рекомендации X.800. Сетевые сервисы безопасности. Аутентификация партнеров по общению. Управление доступом. Конфиденциальность данных. Аутентификация источника данных. Семиуровневая модель OSI. Сетевые механизмы безопасности. Шифрование. Электронная цифровая подпись. Администрирование средств безопасности /лаб/	7	4	0	0	ПК-33	Отчет по лаб. работам
2.3	Тема 2. Стандарты информационной безопасности Краткое содержание: Конфиденциальность данных. Аутентификация источника данных. Семиуровневая модель OSI. Сетевые механизмы безопасности. Шифрование. Электронная цифровая подпись. Администрирование средств безопасности /сп/	7	48	0	0	ПК-33	Устный опрос
<b>Раздел 3. Административный уровень обеспечения информационной безопасности</b>							
3.1	Тема 3. Цели, задачи и содержание административного уровня Краткое содержание: Содержание административного уровня. Дайте определение политики безопасности. Направления разработки политики безопасности. Перечислите составные элементы автоматизированных систем. Субъекты информационных отношений и их роли при обеспечении информационной безопасности <b>знать:</b> классификацию криптоалгоритмов, принцип работы симметричных криптоалгоритмов и криптосистем, принцип работы асимметричных криптоалгоритмов и криптосистем. <b>уметь:</b> создавать симметричные криптоалгоритмы и асимметричные криптоалгоритмы <b>владеть:</b> навыками зашифровки данных симметричными и асимметричными криптоалгоритмами /лек/	7	2	0	0	ПК-33	Конспект
3.2	Тема 3. Разработка политики информационной безопасности Краткое содержание: Основная цель разработки политики безопасности на предприятии. Субъекты и объекты информационных систем и их классификация. Цели и задачи административного уровня обеспечения информационной безопасности. Место политики безопасности в структуре ВНД (внутренней нормативной документации) предприятия /лаб/	7	2	0	0	ПК-33	Отчет по лаб. работам
3.3	Тема 3. Административный уровень обеспечения информационной безопасности Краткое содержание: Субъекты информационных отношений и их роли при обеспечении информационной безопасности /сп/	7	40	0	0	ПК-33	Устный опрос
3.4	Подготовка и проведение зачета с оценкой /ЗаО/	7				ПК-33	Вопросы к зачету с оценкой

**Заочная форма обучения**

Код занятия	Наименования разделов, тем, их краткое содержание и результаты освоения /вид занятия/	Семестр	Часов	Интеракт.	Прак. подг.	Формируемый признак компетенции	Оценочные средства
<b>Раздел 1. Информационная безопасность и уровни ее обеспечения</b>							
1.1	Тема 1. Понятие «Информационная безопасность» Краткое содержание: Информационная безопасность. Защита информации. Основные составляющие информационной безопасности. Доступность, целостность и конфиденциальность информационных ресурсов. Важность и сложность проблемы информационной безопасности. Доктрина информационной безопасности Российской Федерации <b>знать:</b> современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования. <b>уметь:</b> выбрать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты <b>владеть:</b> методами защиты информации и программного обеспечения от несанкционированного доступа и копирования /лек/	7	1	0	0	ПК-33	Конспект
1.2	Тема 1. Составляющие информационной безопасности Краткое содержание: Основные составляющие. Важность проблемы. Понятие информационной безопасности. Защита информации. Основные составляющие информационной безопасности. Основные определения и критерии классификации угроз. Основные угрозы конфиденциальности. /пр/	7	2	0	0	ПК-33	Конспект
1.3	Тема 1. Информационная безопасность и уровни ее обеспечения Краткое содержание: изучить современную ситуацию в области информационной безопасности; категории информационной безопасности; абстрактные модели защиты информации, обзор наиболее распространенных методов "взлома" /ср/	7	40	0	0	ПК-33	Устный опрос
<b>Раздел 2. Стандарты информационной безопасности</b>							
2.1	Тема 2. Стандарты информационной безопасности: "Общие критерии" Краткое содержание: Понятие безопасности информации. Международный стандарт информационной безопасности. Особенности процесса стандартизации в Интернете. Стандарты безопасности в Интернете: SSL (TLS), SET, IPSec. Особенности российского рынка. Государственные стандарты <b>знать:</b> устройство сетевых компонентов: сервера, рабочие станции, среда передачи информации и узлы коммутации сетей <b>уметь:</b> проектировать локальную сеть, объединяя сервера, рабочие станции и среду передачи информации <b>владеть:</b> навыками монтажа локальной сети. /лек/	7	2	0	0	ПК-33	Конспект



2.2	<p>Тема 2. Стандарты информационной безопасности распределенных систем</p> <p>Краткое содержание:  Информационная безопасность распределенных систем. Рекомендации X.800. Сетевые сервисы безопасности. Аутентификация партнеров по общению. Управление доступом. Конфиденциальность данных. Аутентификация источника данных. Семиуровневая модель OSI. Сетевые механизмы безопасности. Шифрование. Электронная цифровая подпись. Администрирование средств безопасности</p> <p>/ лаб /</p>	7	4	0	0	ПК-33	Отчет по лаб. работам
2.3	<p>Тема 2. Стандарты информационной безопасности</p> <p>Краткое содержание: Конфиденциальность данных. Аутентификация источника данных. Семиуровневая модель OSI. Сетевые механизмы безопасности. Шифрование. Электронная цифровая подпись. Администрирование средств безопасности</p> <p>/ср/</p>	7	50	0	0	ПК-33	Устный опрос
<b>Раздел 3. Административный уровень обеспечения информационной безопасности</b>							
3.1	<p>Тема 3. Цели, задачи и содержание административного уровня</p> <p>Краткое содержание:  Содержание административного уровня. Дайте определение политики безопасности. Направления разработки политики безопасности. Перечислите составные элементы автоматизированных систем. Субъекты информационных отношений и их роли при обеспечении информационной безопасности</p> <p><b>знать:</b> классификацию криптоалгоритмов, принцип работы симметричных криптоалгоритмов и криптосистем, принцип работы асимметричных криптоалгоритмов и криптосистем.</p> <p><b>уметь:</b> создавать симметричные криптоалгоритмы и асимметричные криптоалгоритмы</p> <p><b>владеть:</b> навыками зашифровки данных симметричными и асимметричными криптоалгоритмами</p> <p>/лек/</p>	7	1	0	0	ПК-33	Конспект
3.2	<p>Тема 3. Разработка политики информационной безопасности</p> <p>Краткое содержание: Основная цель разработки политики безопасности на предприятии. Субъекты и объекты информационных систем и их классификация. Цели и задачи административного уровня обеспечения информационной безопасности. Место политики безопасности в структуре ВНД (внутренней нормативной документации) предприятия</p> <p>/ пр /</p>	7	2	0	0	ПК-33	Конспект
3.3	<p>Тема 3. Административный уровень обеспечения информационной безопасности</p> <p>Краткое содержание: Субъекты информационных отношений и их роли при обеспечении информационной безопасности</p> <p>/ср/</p>	7	40	0	0	ПК-33	Устный опрос
3.4	Подготовка и проведение зачета с оценкой /ЗаО/	7	4	0	0	ПК-33	Вопросы к зачету с оценкой

## **Перечень применяемых активных и интерактивных образовательных технологий:**

### ***Компьютерная технология обучения***

Основана на использовании информационных технологий в учебном процессе. Реализация данной технологии осуществляется посредством компьютера и иных мультимедийных средств. Использование компьютерных технологий делает учебный процесс современным, познавательным и интересным для обучающихся.

### ***Технология обучения в сотрудничестве***

Технология обучения в сотрудничестве используется в образовательной практике для преодоления последствий индивидуального характера учебной деятельности субъектов и их стремлений исключительно к индивидуальным образовательным достижениям. Она позволяет обогатить опыт и приобрести через учебный труд те навыки совместимой деятельности, которые затем могут стать необходимыми в будущей профессиональной и социальной деятельности в течение жизни. Цель технологии состоит в формировании умений у субъектов образовательного процесса эффективно работать сообща во временных командах и группах и добиваться качественных образовательных результатов.

### ***Лекция-визуализация с применением мультимедийных технологий.***

Систематизация и выделение наиболее существенных элементов информации с помощью мультимедийных технологий.

## **5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ**

Рекомендации по выполнению домашних заданий в режиме СРС

Самостоятельная работа студентов включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме учебной дисциплины студентам, как правило, преподавателем предлагается перечень заданий для самостоятельной работы для учета и оценивания её посредством бально-рейтинговой системы (БРС).

Задания для самостоятельной работы должны исполняться самостоятельно и представляться в установленный преподавателем срок, а также соответствовать установленным требованиям по структуре и его оформлению.

Студентам следует:

- Руководствоваться регламентом СРС, определенным РПД;
- Своевременно выполнять все задания, выдаваемые преподавателем для самостоятельного выполнения;
- Использовать в выполнении, оформлении и сдаче заданий установленные кафедрой требования, для соответствующих видов текущего/промежуточного контроля.

При подготовке к зачету/экзамену, параллельно с лекциями и рекомендуемой литературой, прорабатывать соответствующие научно-теоретические и практико-прикладные аспекты дисциплины.

Рекомендации по работе с источниками информации и литературой:

Любая форма самостоятельной работы студента (подготовка к семинарскому занятию, написание эссе, курсовой работы, доклада и т.п.) начинается с поиска и изучения соответствующих источников информации, включая специализированную и учебную литературу.

Любой выбранный источник информации (сайт, поисковый контент, учебное пособие, монографию, отчет, статью и т.п.) необходимо внимательно просмотреть, определившись с актуальностью тематического состава данного информационного источника:

- в книгах - следует ознакомиться с оглавлением и научно-справочным аппаратом, прочитать аннотацию и предисловие; целесообразно ее пролистать, рассмотреть иллюстрации, таблицы, диаграммы, приложения - такое поверхностное ознакомление позволит узнать, какие главы следует читать внимательно, какие прочитать быстро, какие просто просмотреть на будущее;
- при работе с интернет-источником - целесообразно систематизировать (поименовать в соответствии с наполнением, сохранять в подпапки-разделы и т.п. приемы) или иным образом выделять важную для себя информацию и данные;
- если книга/журнал/компьютер не являются собственностью студента, то целесообразно записывать название книг, статей, номера страниц, которые привлекли внимание, а позже, следует возвратиться к ним, и перечитать нужную информацию более предметно.

Выделяются следующие виды записей при работе с литературой:

- Конспект - краткая схематическая запись основного содержания научной работы. Целью является не переписывание произведения, а выявление его логики, системы доказательств, основных выводов. Хороший конспект должен сочетать полноту изложения с краткостью.
- Цитата - точное воспроизведение текста; заключается в кавычки; точно указывается источник, автор, год издания (или, номер источника из списка литературы - в случае заимствованного цитирования) в прямоугольных скобках.
- Тезисы - концентрированное изложение основных положений прочитанного материала.
- Аннотация - очень краткое изложение содержания прочитанной работы (поисковый образ).
- Резюме – краткие выводы и положения работы, ее концептуальные итоги.

## 6. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ

**6.1. Перечень компетенций с указанием этапов формирования в процессе освоения ОПОП ПК-33 способностью участвовать в разработке новых автоматизированных и автоматических технологий производства продукции и их внедрении, оценке полученных результатов, подготовке технической документации по автоматизации производства и средств его оснащения**

**Недостаточный уровень:**

Не знает новые автоматизированные и автоматические технологии производства продукции и их внедрении, особенности технической документации по автоматизации производства и средств его оснащения;

Не умеет проводить оценку полученных результатов, подготовку технической документации по автоматизации производства и средств его оснащения;

Не владеет способами проведения оценки полученных результатов, подготовку технической документации по автоматизации производства и средств его оснащения;

**Пороговый уровень:**

Посредственно знает новые автоматизированные и автоматические технологии производства продукции и их внедрении, особенности технической документации по автоматизации производства и средств его оснащения;

Посредственно умеет проводить оценку полученных результатов, подготовку технической документации по автоматизации производства и средств его оснащения;

Посредственно способами проведения оценки полученных результатов, подготовку технической документации по автоматизации производства и средств его оснащения;

**Продвинутый уровень:**

Хорошо знает новые автоматизированные и автоматические технологии производства продукции и их внедрении, особенности технической документации по автоматизации производства и средств его оснащения;

Хорошо умеет проводить оценку полученных результатов, подготовку технической документации по автоматизации производства и средств его оснащения;

Хорошо владеет способами проведения оценки полученных результатов, подготовку технической документации по автоматизации производства и средств его оснащения.

**Высокий уровень:**

Отлично знает новые автоматизированные и автоматические технологии производства продукции и их внедрении, особенности технической документации по автоматизации производства и средств его оснащения;

На высшем уровне умеет проводить оценку полученных результатов, подготовку технической документации по автоматизации производства и средств его оснащения;

На высшем уровне владеет способами проведения оценки полученных результатов, подготовку технической документации по автоматизации производства и средств его оснащения.

### 6.2. Шкала оценивания в зависимости от уровня сформированности компетенций

**Уровень сформированности компетенций**

1. Недостаточный: компетенции не сформированы	2. Пороговый: компетенции сформированы	3. Продвинутый: компетенции сформированы	4. Высокий: компетенции сформированы.
Знания отсутствуют	Сформированы базовые структуры знаний.	Знания обширные, системные.	Знания твердые, аргументированные, всесторонние.
Умения не сформированы.	Умения фрагментарны и носят репродуктивный характер.	Умения носят репродуктивный характер применяются к решению типовых заданий.	Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий.
Навыки не сформированы.	Демонстрируется низкий уровень самостоятельности практического навыка.	Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка.

**Описание критериев оценивания**

Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - допускаются принципиальные ошибки при ответе на	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе,	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала;	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание
---	---	---	---

основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкая степень контактности.	недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания, которые следует выполнить.	-способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; - наличие собственной обоснованной позиции по обсуждаемым вопросам. Возможны незначительные оговорки и неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.	основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
0 - 59 баллов	60 - 69 баллов	70 - 89 баллов	90 - 100 баллов
Оценка «незачет», «неудовлетворительно»	Оценка «зачтено», «удовлетворительно»	Оценка «зачтено», «хорошо»	Оценка «зачтено», «отлично»

**Оценочные средства, обеспечивающие диагностику сформированности компетенций, заявленных в рабочей программе по дисциплине (модулю) для проведения промежуточной аттестации**

**ОЦЕНИВАНИЕ УРОВНЯ ЗНАНИЙ: Теоретический блок вопросов, практический блок задач. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и излагать материал, грамотность решения задач.**

**1. Недостаточный уровень**

Не знает современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования; состав и организацию систем информационной безопасности; методы криптографических преобразований, основные стандарты и протоколы шифрования;  
Не умеет выбрать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты; методы криптографических преобразований, основные стандарты и протоколы шифрования;

Не владеет методами защиты информации и программного обеспечения от несанкционированного доступа и копирования; методами криптографических преобразований, основные стандарты и протоколы шифрования;

**2. Пороговый уровень**

Посредственно знает современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования; состав и организацию систем информационной безопасности; методы криптографических преобразований, основные стандарты и протоколы шифрования;

Посредственно умеет выбрать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты; методы криптографических преобразований, основные стандарты и протоколы шифрования;

Посредственно владеет методами защиты информации и программного обеспечения от несанкционированного доступа и копирования; методами криптографических преобразований, основные стандарты и протоколы шифрования;

**3. Продвинутый уровень**

Хорошо знает современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования; состав и организацию систем информационной безопасности; методы криптографических преобразований, основные стандарты и протоколы шифрования;  
Хорошо умеет выбрать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты; методы криптографических преобразований, основные стандарты и протоколы шифрования;

Хорошо владеет методами защиты информации и программного обеспечения от несанкционированного доступа и копирования; методами криптографических преобразований, основные стандарты и протоколы шифрования;

#### 4. Высокий уровень

Отлично знает современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования; состав и организацию систем информационной безопасности; методы криптографических преобразований, основные стандарты и протоколы шифрования; В совершенстве умеет выбрать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты; методы криптографических преобразований, основные стандарты и протоколы шифрования;

В совершенстве владеет методами защиты информации и программного обеспечения от несанкционированного доступа и копирования; методами криптографических преобразований, основные стандарты и протоколы шифрования.

Рейтинг обучающегося в семестре по дисциплине складывается из рейтинговых баллов, которыми преподаватель в течение семестра оценивает посещение учебных занятий, его текущую работу на занятиях и самостоятельную работу, результаты текущих тестов, устных опросов, премиальных и штрафных баллов. Рейтинг обучающегося при прохождении промежуточной аттестации по дисциплине складывается из оценки в рейтинговых баллах ответа на зачете.

В случае, если сумма рейтинговых баллов, полученных при прохождении промежуточной аттестации составляет от 0 до 9 баллов, то зачет НЕ СДАН, независимо от итогового рейтинга по дисциплине. В случае, если сумма рейтинговых баллов, полученных при прохождении промежуточной аттестации находится в пределах от 10 до 30 баллов, то зачет СДАН, и результат сдачи определяется в зависимости от итогового рейтинга по дисциплине в соответствии с утвержденной шкалой перевода из 100-балльной шкалы оценивания в 5- балльную.

Для приведения рейтинговой оценки по дисциплине по 100-балльной шкале к аттестационной по 5-балльной шкале в соответствии с Положением о балльно-рейтинговой системе оценки успеваемости студентов федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет технологий и управления имени К.Г. Разумовского (Первый казачий университет) используется следующая шкала:

Аттестационная оценка по дисциплине	Рейтинговая оценка по дисциплине
"ОТЛИЧНО"	90 - 100 баллов
"ХОРОШО"	70 - 89 баллов
"УДОВЛЕТВОРИТЕЛЬНО"	60 - 69 баллов
"НЕУДОВЛЕТВОРИТЕЛЬНО"	менее 60 баллов
"ЗАЧТЕНО"	более 60 баллов
"НЕ ЗАЧТЕНО"	менее 60 баллов

### 6.3. Оценочные средства текущего контроля

#### Оценочные средства для устного опроса

##### Тема 1. Понятие «Информационная безопасность»

Основные составляющие информационной безопасности.

Доступность, целостность и конфиденциальность информационных ресурсов.

Важность и сложность проблемы информационной безопасности.

Доктрина информационной безопасности Российской Федерации

Основные определения и критерии классификации угроз.

Основные угрозы конфиденциальности.

##### Тема 2. Стандарты информационной безопасности: "Общие критерии"

Понятие безопасности информации.

Международный стандарт информационной безопасности.

Особенности процесса стандартизации в Интернете.

Стандарты безопасности в Интернете: SSL (TLS), SET, IPSec.

Особенности российского рынка.

Государственные стандарты

##### Тема 3. Цели, задачи и содержание административного уровня

Содержание административного уровня.

Определение политики безопасности.

Направления разработки политики безопасности.

Составные элементы автоматизированных систем.

Субъекты информационных отношений и их роли при обеспечении информационной безопасности  
Основная цель разработки политики безопасности на предприятии.  
Субъекты и объекты информационных систем и их классификация.  
Цели и задачи административного уровня обеспечения информационной безопасности.  
Место политики безопасности в структуре ВНД (внутренней нормативной документации) предприятия

#### 6.4 Оценочные средства для проведения промежуточной аттестации

##### Перечень вопросов к зачету

1. Основные задачи защиты информации. Общие принципы построения криптографических алгоритмов.
2. Типы алгоритмов шифрования. Стойкость алгоритмов.
3. Классификация алгоритмов. Классификация угроз. Концепция теоретической и практической стойкости К. Шеннона.
4. Алгоритмы блочного шифрования. Принципы построения блочных шифров. Схема Фейстеля.
5. Примеры блочных алгоритмов (DES, ГОСТ 28147-89).
6. Режимы использования блочных шифров. Методы анализа алгоритмов блочного шифрования, рекомендации по использованию
7. Алгоритмы поточного шифрования. Принципы построения поточных шифросистем. Линейные регистры сдвига.
8. Алгоритмы поточного шифрования. Усложнение рекуррентных последовательностей. Синхронизация поточных шифросистем.
9. Примеры поточных шифров (A5, SEAL). Методы анализа поточных шифров
10. Ассиметричные криптосистемы. Основные принципы. Сложные задачи.
11. Модулярная арифметика. Кольца вычетов.
12. Шифросистемы на основе рюкзачной системы. Стойкость.
13. Шифросистемы RSA, Эль-Гамала. Стойкость.
14. Хэш-функции. Общие сведения. Типы функций хэширования. Стандарты.
15. Возможные атаки на функции хэширования. Требования к хэш-функциям. Стойкость.
16. Электронная цифровая подпись. Общие положения. ЦП на основе алгоритмов с открытыми ключами.
17. Цифровая подпись Эль-Гамала. Схема RSA. Примеры (DSS-федеральный стандарт США, ГОСТ-Р 34.10-94).
18. Криптографические протоколы. Общие сведения.
19. Криптографические протоколы. Формальные методы анализа, BAN-логика.
20. Протоколы аутентификации. Специальные криптографические протоколы. Примеры.
21. Методы аутентификации. Типы угроз и меры по противодействию.
22. Одноразовые пароли. Метод «запрос-ответ».
23. Биометрические методы аутентификации.
24. Криптографические методы аутентификации. Методы, основанные на свойствах симметричных криптосистем.
25. Криптографические методы аутентификации. Методы, основанные на свойствах ассиметричных криптосистем.
26. Анализ протоколов аутентификации.
27. Модель KERBEROS.
28. Контроль целостности информации. CRC-код. Способы формирования. Надёжность, стойкость
29. Криптографические методы контроля целостности информации. Основные подходы (MAC, MDC). Имитозащита информации.
30. Управление ключами. Жизненный цикл ключей. Генерация ключей. Ключевое пространство.
31. Управление ключами. Хранение, распределение, использование, уничтожение, компрометация ключей. Депонирование ключей. Стандарт EES.
32. Квантово-криптографический протокол открытого распределения ключей. Квантовый канал и его свойства.
33. Сущность понятия "защищаемая информация"
34. Разновидность защищаемой информации
35. Носители защищаемой информации
36. Понятие ИБ. Составляющие ИБ.
37. Понятие «государственная тайна», сведения, составляющие государственную тайну. Основные положения Закона РФ "О государственной тайне".
38. Коммерческая тайна и ее особенности. Основные положения Закона РФ «О коммерческой тайне»
39. Российское законодательство в области ИБ.
40. Государственная система защиты информации
41. Защищенные информационные системы. Основные понятия.
42. Понятие угроз ИБ. Критерии их классификации.
43. Административно-правовые методы защиты информации. Политика информационной безопасности: основные положения.

- 44 Физические (организационные) методы обеспечения информационной безопасности. Основные классы мер организационного уровня обеспечения информационной безопасности.
- 45 DLP-системы: назначение, принципы построения, функциональные возможности.
- 46 Назначение криптографических методов защиты информации. Классификация методов криптографического преобразования информации.
- 47 Классификация шифров замены. Примеры.
- 48 Классификация шифров перестановки. Примеры.
- 49 Аналитические методы шифрования. Пример.
- 50 Методы гаммирования. Стандарты шифрования.
- 51 Роль стандартов ИБ. Основные понятия и определения.
- 52 Критерии безопасности компьютерных систем «Оранжевая книга».
- 53 Гармонизированные критерии Европейских стран.
- 54 Стандарт ISO / IEC 15408.
- 55 Международный стандарт безопасности информационных систем ISO 17799.
- 56 Открытый стандарт COBIT
- 57 Аудит информационной безопасности: цель, виды, методики.
- 58 Основные этапы проведения аудита информационной безопасности.
- 59 Учетные записи и группы пользователей. Стратегия управления учетными записями в Active Directory
- 60 Дисковые квоты.
- 61 Профили пользователей.
- 62 Понятие и назначение реестра Windows. Назначение корневых разделов реестра Windows.
- 63 Команды работы с реестром.
- 64 Настройка политик безопасности в Windows: политика учетных записей, политика паролей, политика аудита.
- 65 Обеспечение хранения данных в Windows Server 2008: теневые копии, архивы.
- 66 Информационная безопасность распределенных систем. Рекомендации X.800.

#### **6.5. Примерная тематика курсовых работ (проектов)**

Учебным планом не предусмотрено

#### **6.6. Методические указания для обучающихся по освоению дисциплины (модуля)**

Цель данных указаний – оптимизировать организацию процесса изучения дисциплины студентом, а также выполнение некоторых форм и навыков самостоятельной работы.

##### **Рекомендации по подготовке к лекционным занятиям**

Изучение дисциплины требует систематического и последовательного накопления знаний, следовательно, пропуски отдельных тем не позволяют глубоко освоить предмет. Именно поэтому контроль над систематической работой студентов всегда находится в центре внимания кафедры.

Студентам необходимо:

- перед каждой лекцией просматривать РПД и предыдущую лекцию, что, возможно, позволит сэкономить трудозатраты на конспектировании новой лекции (в случае, когда предыдущий материал идет как опорный для последующего), ее основных разделов и т.п.;

- на некоторые лекции приносить вспомогательный материал на бумажных носителях, рекомендуемый лектором (таблицы, графики, схемы). Данный материал необходим непосредственно для лекции;

- при затруднениях в восприятии лекционного материала, следует обратиться к рекомендуемым и иным литературным источникам и разобраться самостоятельно. Если разобраться в материале все же не удалось, то существует график консультаций преподавателя, когда можно обратиться к нему за пояснениями или же прояснить этот вопрос у более успевающих студентов своей группы (потока), а также на практических занятиях. Важно не оставлять масштабных «белых пятен» в освоении материала.

##### **Рекомендации по подготовке к лабораторным работам**

В ходе лабораторной работы необходимо выполнить задания на компьютере и ответить на вопросы к лабораторным работам.

При подготовке к лабораторным занятиям студент должен придерживаться следующей технологии:

- внимательно изучить основные вопросы темы и план лабораторной работы, определить место темы занятия в общем содержании, ее связь с другими темами;
- найти и проработать соответствующие разделы в рекомендованных нормативных документах, основной и дополнительной литературе;
- продумать развернутые ответы на вопросы, опираясь на лекционные материалы, расширяя и дополняя их данными из основной и дополнительной литературы.

## **7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

### **7.1. Рекомендуемая литература**

#### **7.1.1. Основная литература**

- 1 Сычев Ю.Н. Защита информации и информационная безопасность [Электронный ресурс]: Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2021. - 201 с. – Режим доступа: <http://znanium.com/catalog/document?id=366835УП: 150304-АТППо-21.plx> стр. 29
- 2 Л.1.2 Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации [Электронный ресурс]: Учебное пособие. - Москва: Издательский Центр РИО, 2021. - 336 с. – Режим доступа: <http://znanium.com/catalog/document?id=364911>

#### **7.1.2. Дополнительная литература**

- 3 Л.1.3 Глинская Е.В., Чичварин Н.В. Информационная безопасность конструкций ЭВМ и систем [Электронный ресурс]: Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2021. - 118 с. – Режим доступа: <http://znanium.com/catalog/document?id=364725>
- 4 Л.1.4 Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей [Электронный ресурс]: Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2021. - 416 с. – Режим доступа: <http://znanium.com/catalog/document?id=364622>

### **7.2. Лицензионное и свободно распространяемое программное обеспечение в том числе отечественного производства**

1. Операционная система MS Windows;
2. MSOffice 2010
3. WIN HOME 10 Russian OLP NL AcademicEdition Legalization

### **7.3. Перечень профессиональных баз данных, информационных справочных систем и ресурсов сети Интернет**

#### **7.3.1. Электронно-библиотечные системы**

1. Электронно-библиотечная система "Лань". Режим доступа: <https://e.lanbook.com/>
2. Электронно-библиотечная система "Университетская библиотека онлайн". Режим доступа: <https://biblioclub.ru/>
3. Электронно-библиотечная система "Znanium.com". Режим доступа: <https://znanium.com/>
4. Национальный цифровой ресурс "РУКОНТ". Режим доступа: <https://rucont.ru/>
5. Научная электронная библиотека "eLIBRARY.RU". Режим доступа: <https://www.elibrary.ru/>

#### **7.3.2. Интернет-ресурсы**

1. <http://school-collection.edu.ru/> - Федеральное хранилище «Единая коллекция цифровых образовательных ресурсов»
2. <http://window.edu.ru/>- Портал «Единое окно доступа к образовательным ресурсам»
3. <http://acmp.ru/>– Школа программиста.

## **8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**

Лаборатория «Робототехники и систем программного управления».

Учебная аудитория для проведения занятий лекционного типа; занятий лабораторного и практического типа; для курсового проектирования (выполнения курсовых работ); для проведения групповых и индивидуальных консультаций; для текущего контроля и промежуточной аттестации.

Рабочие места обучающихся; Рабочее место преподавателя; Ноутбук; Проектор переносной; Экран переносной; Классная доска; 17 рабочих мест обучающихся оснащенные ПЭВМ с подключением к сети интернет и обеспечением доступа в электронную информационно-образовательную среду Университета. Учебно-лабораторный стенд «Автоматизация регулирования основных технологических параметров». Учебно-лабораторный стенд «Автономная автоматизированная система отопления»

Адрес: 453850, Республика Башкортостан, г. Мелеуз, ул. Смоленская, д. 34: аудитория1-122

## **9. ОРГАНИЗАЦИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ**

Организация образовательного процесса для лиц с ограниченными возможностями осуществляется в соответствии с «Методическими рекомендациями по организации образовательного процесса для инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащённости образовательного процесса» Министерства образования и науки РФ от 08.04.2014г. № АК-44/05вн. В образовательном процессе используются социально-активные и рефлексивные методы обучения, технологии социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими студентами, создании комфортного психологического климата в студенческой группе. Студенты с ограниченными возможностями здоровья, в отличие от остальных студентов, имеют свои специфические особенности восприятия, переработки материала. Подбор и разработка



учебных материалов производятся с учетом индивидуальных особенностей. Предусмотрена возможность обучения по индивидуальному графику, при составлении которого возможны различные варианты проведения занятий: в академической группе и индивидуально, на дому с использованием дистанционных образовательных технологий.

**Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы**

Руководитель ОПОП

\_\_\_\_\_  
ФИО, должность, ученая степень, звание                      Подпись  
Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры  
Информационные технологии и системы управления  
Протокол от \_\_\_\_\_ 202\_\_ г. № \_\_

\_\_\_\_\_  
ФИО, должность, ученая степень, звание                      Подпись  
Рабочая программа согласована на заседании выпускающей кафедры  
Информационные технологии и системы управления  
Протокол от \_\_\_\_\_ 202\_\_ г. № \_\_

\_\_\_\_\_  
ФИО, должность, ученая степень, звание                      Подпись

**Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы**

Руководитель ОПОП

\_\_\_\_\_  
ФИО, должность, ученая степень, звание                      Подпись  
Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры  
Информационные технологии и системы управления  
Протокол от \_\_\_\_\_ 202\_\_ г. № \_\_

\_\_\_\_\_  
ФИО, должность, ученая степень, звание                      Подпись  
Рабочая программа согласована на заседании выпускающей кафедры  
Информационные технологии и системы управления  
Протокол от \_\_\_\_\_ 202\_\_ г. № \_\_

\_\_\_\_\_  
ФИО, должность, ученая степень, звание                      Подпись

**Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы**

Руководитель ОПОП

\_\_\_\_\_  
ФИО, должность, ученая степень, звание                      Подпись  
Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры  
Информационные технологии и системы управления  
Протокол от \_\_\_\_\_ 202\_\_ г. № \_\_

\_\_\_\_\_  
ФИО, должность, ученая степень, звание                      Подпись  
Рабочая программа согласована на заседании выпускающей кафедры  
Информационные технологии и системы управления  
Протокол от \_\_\_\_\_ 202\_\_ г. № \_\_

\_\_\_\_\_  
ФИО, должность, ученая степень, звание                      Подпись

**Актуализация с учетом развития науки, техники, культуры, экономики, техники, технологий и социальной сферы**

Руководитель ОПОП

\_\_\_\_\_  
ФИО, должность, ученая степень, звание                      Подпись  
Рабочая программа актуализирована, обсуждена и одобрена на заседании обеспечивающей кафедры  
Информационные технологии и системы управления  
Протокол от \_\_\_\_\_ 202\_\_ г. № \_\_

\_\_\_\_\_  
ФИО, должность, ученая степень, звание                      Подпись  
Рабочая программа согласована на заседании выпускающей кафедры  
Информационные технологии и системы управления  
Протокол от \_\_\_\_\_ 202\_\_ г. № \_\_

\_\_\_\_\_  
ФИО, должность, ученая степень, звание                      Подпись