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.06.02 Информационная безопасность 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.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 00940BA2D772BADC6721A08E042746B11B
Владелец: Кузнецова Елена Валентиновна
Действителен: с 07.07.2023 до 29.09.2024

Мелеуз 2023

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

Рабочая программа дисциплины (модуля) «Информационная безопасность 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. Одинокова _____

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. Одинокова _____

СОДЕРЖАНИЕ

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**	
Недель	18 1/6			
Вид занятий	УП	РП	УП	РП
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**	
Недель	2 5/6			
Вид занятий	УП	РП	УП	РП
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 «Информационная безопасность 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:

- развертывать 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 компетенций	Оценочные средства
	Раздел 1. Информационная безопасность и уровни ее обеспечения						
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 **знать:** современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования. **уметь:** выбрать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты **владеть:** 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
	Раздел 2. Стандарты информационной безопасности						
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 **знать:** устройство сетевых компонентов: сервера, рабочие станции, среда передачи информации и узлы коммутации сетей	7	4	0	0	ПК-33	Конспект

	уметь: проектировать локальную сеть, объединяя сервера, рабочие станции и среду передачи информации **владеть:** 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 /ср/	7	48	0	0	ПК-33	Устный опрос
	Раздел 3. Административный уровень обеспечения информационной безопасности						
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 **знать:** классификацию криптоалгоритмов, принцип работы симметричных криптоалгоритмов и криптосистем, принцип работы асимметричных криптоалгоритмов и криптосистем. **уметь:** создавать симметричные криптоалгоритмы и асимметричные криптоалгоритмы **владеть:** 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 /ср/	7	40	0	0	ПК-33	Устный опрос
3.4	Подготовка и проведение зачета с оценкой /Зачет с оценкой/	7	0	0	0	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 компетенций	Оценочные средства
	Раздел 1. Информационная безопасность и уровни ее обеспечения						
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 **знать:** современные методы обеспечения целостности и защиты информации и программных средств от несанкционированного доступа и копирования. **уметь:** выбрать соответствующие организационные и программно-аппаратные средства для организации систем информационной защиты **владеть:** 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
	Раздел 2. Стандарты информационной безопасности						
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 **знать:** устройство сетевых компонентов: сервера, рабочие станции, среда передачи информации и узлы коммутации сетей **уметь:** проектировать локальную сеть, объединяя сервера, рабочие станции и среду передачи информации **владеть:** навыками монтажа локальной сети.	7	2	0	0	ПК-33	Конспект

	/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 /ср/	7	50	0	0	ПК-33	Устный опрос
	Раздел 3. Административный уровень обеспечения информационной безопасности						
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 **знать:** классификацию криптоалгоритмов, принцип работы симметричных криптоалгоритмов и криптосистем, принцип работы асимметричных криптоалгоритмов и криптосистем. **уметь:** создавать симметричные криптоалгоритмы и асимметричные криптоалгоритмы **владеть:** навыками зашифровки данных симметричными и асимметричными криптоалгоритмами /лек/	7	1	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 / пр /	7	2	0	0	ПК-33	Конспект
3.3	Тема 3. Административный уровень обеспечения информационной безопасности Краткое содержание: Субъекты информационных отношений и их роли при обеспечении информационной безопасности /ср/	7	40	0	0	ПК-33	Устный опрос
3.4	Подготовка и проведение зачета с оценкой /Зачет с оценкой/	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 основные	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

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.	и явлений, точное знание 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. Основные виды и источники атак на информацию

1. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.
2. Основные понятия информационной безопасности.
3. Структура понятия информационная безопасность.
4. Система защиты информации и ее структура.
5. Экономическая информация как товар и объект безопасности.
6. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
7. Персональные данные и их защита.
8. Информационные угрозы, их виды и причины возникновения.
9. Информационные угрозы для государства.
10. Информационные угрозы для компании.
11. Информационные угрозы для личности (физического лица).

Тема 2. Сетевая безопасность

1. Защита информации в Интернете.
2. Электронная почта и ее защита.
3. Защита от компьютерных вирусов.
4. «Больные» мобильники и их «лечение».
5. Популярные антивирусные программы и их классификация.
6. Организация системы защиты информации экономических объектов

Тема 3. Криптография

1. Классификация криптоалгоритмов
2. Симметричные криптоалгоритмы
3. Симметричные криптосистемы
4. Асимметричные криптоалгоритмы

Тема 4. ПО и информационная безопасность

1. Политика безопасности и ее принципы.
2. Фрагментарный и системный подход к защите информации.
3. Методы и средства защиты информации.
4. Организационное обеспечение ИБ.
5. Организация конфиденциального делопроизводства.
6. Комплекс организационно-технических мероприятий по обеспечению защиты информации.
7. Инженерно-техническое обеспечение компьютерной безопасности.

Тема 5. Комплексная система безопасности

1. План обеспечения непрерывной работы и восстановления функционирования автоматизированной информационной системы.
2. Управление информационной безопасности на государственном уровне.
3. Аудит ИБ автоматизированных банковских систем.
4. Электронная коммерция и ее защита.
5. Менеджмент и аудит информационной безопасности на уровне предприятия.
6. Информационная безопасность предпринимательской деятельности.

Типовая структура отчета по лабораторной работе

1. Тема лабораторной работы
2. Цель и задачи лабораторной работы
3. Результаты проведенной работы
4. Заключение по лабораторной работе.

6.4 Оценочные средства для проведения промежуточной аттестации

Перечень вопросов к зачету

1 Сущность понятия "защищаемая информация"
2 Разновидность защищаемой информации
3 Носители защищаемой информации
4 Понятие ИБ. Составляющие ИБ.
5 Понятие «государственная тайна», сведения, составляющие государственную тайну. Основные положения Закона РФ "О государственной тайне".
6 Коммерческая тайна и ее особенности. Основные положения Закона РФ «О коммерческой тайне»
7 Российское законодательство в области ИБ.
8 Государственная система защиты информации
9 Защищенные информационные системы. Основные понятия.
10 Понятие угроз ИБ. Критерии их классификации.
11 Административно-правовые методы защиты информации. Политика информационной безопасности: основные положения.
12 Физические (организационные) методы обеспечения информационной безопасности. Основные классы мер организационного уровня обеспечения информационной безопасности.
13 DLP-системы: назначение, принципы построения, функциональные возможности.
14 Назначение криптографических методов защиты информации. Классификация методов криптографического преобразования информации.
15 Классификация шифров замены. Примеры.
16 Классификация шифров перестановки. Примеры.
17 Аналитические методы шифрования. Пример.
18 Методы гаммирования. Стандарты шифрования.
19 Роль стандартов ИБ. Основные понятия и определения.
20 Критерии безопасности компьютерных систем «Оранжевая книга».
21 Гармонизированные критерии Европейских стран.
22 Стандарт ISO / IEC 15408.
23 Международный стандарт безопасности информационных сис¬тем ISO 17799.
24 Открытый стандарт COBIT
25 Аудит информационной безопасности: цель, виды, методики.
26 Основные этапы проведения аудита информационной безопасности.
27 Учетные записи и группы пользователей. Стратегия управления учетными записями в Active Directory
28 Дисковые квоты.

29 Профили пользователей.
30 Понятие и назначение реестра Windows. Назначение корневых разделов реестра Windows.
31 Команды работы с реестром.
32 Настройка политик безопасности в Windows: политика учетных записей, политика паролей, политика аудита.
33 Обеспечение хранения данных в Windows Server 2008: теневые копии, архивы.
34 Информационная безопасность распределенных систем. Рекомендации X.800.

Перечень вопросов к экзамену

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 реккурентных 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-Гамаля. 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-Гамаля. 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 ассимметричных криптосистем.
26. Анализ протоколов аутентификации.
27. Модель KERBEROS.
28. Контроль целостности информации. CRC-код. Способы формирования. НадJжность, 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.

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 практическим занятиям

Студентам следует:

- приносить с собой рекомендованную преподавателем к занятию литературу;

- до очередного практического занятия, по рекомендованным литературным источникам проработать теоретический материал, соответствующей темы занятия;

- при подготовке к практическим занятиям рекомендуется использовать не только лекции, учебную литературу, но и нормативно-правовую документацию в случае её актуальности по теме, а также материалы прикладных тематических исследований;

- теоретический материал следует соотносить с прикладным, так как в них могут применяться различные подходы, методы и инструментарий, которые не всегда отражены в лекции или рекомендуемой учебной литературе;

- в начале практических занятий, определить с преподавателем вопросы по разрабатываемому материалу, вызывающему особые затруднения в его понимании, освоении, необходимых при решении поставленных на занятии задач;

- в ходе занятий формулировать конкретные вопросы/ответы по существу задания;

- на занятиях, доводить каждую задачу до окончательного/логического решения, демонстрируя понимание проведенных расчетов (анализа, ситуаций).

Студентам, пропустившим занятия (независимо от причин), не имеющие письменного выполнения практической/ лабораторной работы или иного задания преподавателя, или не подготовившиеся к данному практическому занятию, рекомендуется отчитаться преподавателю по пропущенным темам занятий одним из установленных методов (самостоятельно переписанный конспект, реферат-отработка, выполненная лабораторно-практическая работа/задание и т.п.), не позже соответствующего следующего занятия.

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 оснащенности 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