СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет ***Математики и информационных технологий***
Кафедра ***Математического моделирования***

Аннотация рабочей программы дисциплины (модуля)

дисциплина ***Б1.О.22 Программно-аппаратные средства защиты информации***

обязательная часть

Направление

10.03.01 ***Информационная безопасность***
код наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очно-заочная

Для поступивших на обучение в
2023 г.

Стерлитамак 2023

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)
ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;	ОПК-2.1. Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями.	Обучающийся должен: уметь оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями
	ОПК-2.2. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	Обучающийся должен: уметь выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.
	ОПК-2.3. Обладает навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	Обучающийся должен: владеть навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.

2. Цели и место дисциплины (модуля) в структуре образовательной программы

Цели изучения дисциплины:
Дисциплина имеет цель:
обучить студентов принципам обеспечения информационной безопасности, подходам к анализу его информационной инфраструктуры и решению задач обеспечения информационной безопасности компьютерных систем;
содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.
Названная дисциплина является базовой для изучения других дисциплин специальности «Компьютерная безопасность», а также будет использована при выполнении курсовых и дипломных работ.

Задачи освоения дисциплины: дать основы: методологии создания систем защиты информации; методов, средств и приемов ведения информационных войн; обеспечения информационной безопасности компьютерных систем.

Дисциплина изучается на 4 курсе в 7 семестре

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 5 зач. ед., 180 акад. ч.

Объем дисциплины	**Всего часов**
	Очно-заочная обучения
Общая трудоемкость дисциплины	180
Учебных часов на контактную работу с преподавателем:	
лекций	24
практических (семинарских)	28
лабораторных	28
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	
дифференцированный зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	99,8

Формы контроля	**Семестры**
дифференцированный зачет	7

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

№ п/п	**Наименование раздела / темы дисциплины**	**Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах)**			
		Контактная работа с преподавателем			**СР**
		Лек	**Пр/Сем**	**Лаб**	
1	**Модуль 1**	**10**	**10**	**12**	**38,8**
1.1	Предмет и задачи программно-аппаратной защиты	3	4	3	12
1.2	Стандарты безопасности	4	2	5	15
1.3	Защита от несанкционированного доступа (НСД) в информационных системах	3	4	4	11,8
2	**Модуль 2**	**14**	**18**	**16**	**61**
2.1	Защищенная автоматизированная система	1	3	5	15
2.2	Принципы программно- аппаратной защиты информации от	4	4	3	13

	несанкционированного доступа				
2.3	Дестабилизирующее воздействие на объекты защиты	3	5	4	12
2.4	Основные методы обеспечения информационной безопасности	4	3	2	10
2.5	Средства защиты информации от несанкционированного доступаБезымянный	2	3	2	11
	Итого	**24**	**28**	**28**	**99,8**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Модуль 1**	
1.1	Предмет и задачи программно-аппаратной защиты	Предмет и задачи программно-аппаратной защиты информации. Основные понятия программно-аппаратной защиты информации
1.2	Стандарты безопасности	Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Профили защиты программных и программно-аппаратных средств (межсетевых экранов, средств контроля съемных машинных носителей информации, средств доверенной загрузки, средств антивирусной защиты)
1.3	Защита от несанкционированного доступа (НСД) в информационных системах	Классификация автоматизированных систем и требования по защите информации. Структура системы защиты информации от НСД. Назначение и функции элементов. Модели управления доступом.
2	**Модуль 2**	
2.1	Защищенная автоматизированная система	Автоматизация процесса обработки информации. Понятие автоматизированной системы. Особенности автоматизированных систем в защищенном исполнении.
2.2	Принципы программно-аппаратной защиты информации от несанкционированного доступа	Понятие несанкционированного доступа к информации.
2.3	Дестабилизирующее воздействие на объекты защиты	Источники дестабилизирующего воздействия на объекты защиты
2.4	Основные методы обеспечения информационной безопасности	Основные понятия криптографической защиты информации. Симметричные

		криптографические системы. Ассиметричные криптографические системы. Идентификация и аутентификация. Разграничение и контроль доступа к информации. Технологии межсетевых экранов. Виртуальные частные сети (VPN). Методы обнаружения вторжений (атак).
2.5	Средства защиты информации от несанкционированного доступаБезымянный	Перс. средства аутентификации данных - USB-ключи и смарт-карты eToken. Система защиты от НСД «Dallas Lock». Электронный замок "Соболь". Система защиты конф. информации и персональных данных «Secret Disk». Программно - аппаратный комплекс средств защиты информации от НСД “Аккорд»

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Модуль 1**	
1.1	Предмет и задачи программно-аппаратной защиты	Классификация методов и средств программно-аппаратной защиты информации.
1.2	Стандарты безопасности	Защита информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами
1.3	Защита от несанкционированного доступа (НСД) в информационных системах	Персональные средства аутентификации и защищенного хранения данных - USB-ключи и смарт-карты eToken. Лабораторная работа № 1. (2 часа). Назначение, возможности и порядок работы с персональными средствами аутентификации и защищённого хранения данных (USB-ключи и смарт-карты eToken).
2	**Модуль 2**	
2.1	Защищенная автоматизированная система	Методы создания безопасных систем. Проектирование гарантированно защищенных систем.
2.2	Принципы программно- аппаратной защиты информации от несанкционированного доступа	Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам.
2.3	Дестабилизирующее воздействие на объекты защиты	Способы воздействия на информацию.
2.4	Основные методы обеспечения информационной безопасности	Виды угроз информационной безопасности Российской Федерации. Лабораторная работа № 2. (6 часов). «Выработка концептуальных основ

		деятельности по обеспечению информационной безопасности предприятия»
2.5	Средства защиты информации от несанкционированного доступаБезымянный	Система защиты от НСД «Dallas Lock». Лабораторная работа № 3. (4 часа). Назначение и возможности системы защиты от НСД «Dallas Lock».

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Модуль 1**	
1.1	Предмет и задачи программно-аппаратной защиты	Классификация методов и средств программно-аппаратной защиты информации
1.2	Стандарты безопасности	Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами
1.3	Защита от несанкционированного доступа (НСД) в информационных системах	Классификация автоматизированных систем и требования по защите информации. Документы Гостехкомиссии при Президенте РФ. Концепции защиты автоматизированных систем и средств вычислительной техники. Классификация информационных систем по уровню их защищенности. Требования к информационным системам по обеспечению безопасности информации
2	**Модуль 2**	
2.1	Защищенная автоматизированная система	Основные виды автоматизированных систем в защищенном исполнении. Методы создания безопасных систем. Методология проектирования гарантированно защищенных систем.
2.2	Принципы программно-аппаратной защиты информации от несанкционированного доступа	Понятие несанкционированного доступа к информации. Основные подходы к защите информации от несанкционированного доступа. Организация доступа к файлам, контроль доступа и разграничение доступа, иерархический доступ к файлам. Фиксация доступа к файлам
2.3	Дестабилизирующее воздействие на объекты защиты	Способы воздействия на информацию. Причины и условия дестабилизирующего воздействия на информацию
2.4	Основные методы обеспечения информационной безопасности	Определяются предмет и задачи криптографии, формулируются основополагающие определения и требования к криптографическим системам защиты информации, дается историческая справка об основных этапах развития криптографии как науки. Рассматривается пример простейшего шифра, на основе которого

		поясняются сформулированные понятия и тезисы.
2.5	Средства защиты информации от несанкционированного доступаБезымянный	Персональные средства аутентификации и защищённого хранения данных - USB-ключи и смарт-карты eToken. Назначение, возможности и порядок работы с персональными средствами аутентификации и защищённого хранения данных (USB-ключи и смарт-карты eToken).