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 ***Программно-аппаратные средства защиты информации***

Блок Б1, базовая часть, Б1.Б.29
цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

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

Программа

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

Форма обучения

Очная

Для поступивших на обучение в
2020 г.

Стерлитамак 2023

1. Перечень планируемых результатов обучения по дисциплине (модулю)

1.1. Перечень планируемых результатов освоения образовательной программы

Выпускник, освоивший программу высшего образования, в рамках изучаемой дисциплины, должен обладать компетенциями, соответствующими видам профессиональной деятельности, на которые ориентирована программа:

Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)
Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Формируемая компетенция (с указанием кода)	Этапы формирования компетенции	Планируемые результаты обучения по дисциплине (модулю)
Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)	1 этап: Знания	Обучающийся должен знать: - место и роль систем управления версиями в процессе разработки программного обеспечения; - принципы использования современных систем управления версиями.
	2 этап: Умения	Обучающийся должен уметь: - основные тенденции развития рынка программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем управления организацией; - условия создания и эксплуатации программно-аппаратных средств обеспечения информационной безопасности автоматизированных систем управления коммерческой организацией; - безопасные сетевые технологии, в которых используются программно-аппаратные средств обеспечения информационной безопасности; принципы функционирования и обеспечения защиты программно-аппаратных средств информационной

		безопасности;
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: методами установки и настройки программных, программно-аппаратных и технических средств защиты информации.
Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)	1 этап: Знания	Обучающийся должен знать: информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
	2 этап: Умения	Обучающийся должен уметь: использовать современные системы управления версиями в процессе работы над индивидуальным и командным проектами.
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: - навыками работы в системе Git. Должен демонстрировать способность и готовность: - использовать полученные знания и навыки в дальнейшей учебной и профессиональной деятельности.

2. Место дисциплины (модуля) в структуре образовательной программы

Данная учебная дисциплина включена в раздел "Б1.В.ДВ.4 Дисциплины (модули)" основной профессиональной образовательной программы 10.03.01 "Информационная безопасность (Безопасность компьютерных систем)" и относится к дисциплинам по выбору.

Дисциплина изучается на 3 курсе в 6 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 4 зач. ед., 144 акад. ч.

Объем дисциплины	**Всего часов**
	Очная форма обучения
Общая трудоемкость дисциплины	144
Учебных часов на контактную работу с преподавателем:	
лекций	12
практических (семинарских)	18

лабораторных	18
другие формы контактной работы (ФКР)	1,2
Учебных часов на контроль (включая часы подготовки):	34,8
курсовая работа	
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР):	60
курсовая работа	

Формы контроля	Семестры
курсовая работа	6
экзамен	6

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	**Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности.**	**8**	**12**	**12**	**39**
1.1	Введение. Основные понятия.	2	2	2	10
1.2	Стандарты и спецификации в области ИБ. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.	2	4	5	9
1.3	Категории и модели информационной безопасности	2	4	3	10
1.4	Идентификация и аутентификация пользователей. Понятие несанкционированного доступа.	2	2	2	10
2	**Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем**	**4**	**6**	**6**	**21**
2.1	Программно-аппаратные средства шифрования.	2	2	2	12
2.2	Защита компонентов ПЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим	2	4	4	9

	носителям.				
	Итого	**12**	**18**	**18**	**60**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности.**	
1.1	Введение. Основные понятия.	Основные понятия в области обеспечения безопасности информации
1.2	Стандарты и спецификации в области ИБ. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.	Технические средства защиты информации от несанкционированного доступа
1.3	Категории и модели информационной безопасности	Категории и модели информационной безопасности
1.4	Идентификация и аутентификация пользователей. Понятие несанкционированного доступа.	Понятие несанкционированного доступа. Тип:
2	**Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем**	
2.1	Программно-аппаратные средства шифрования.	Основные виды программно-аппаратных средств защиты информации.
2.2	Защита компонентов ПЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.	способность определять информационные ресурсы

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности.**	
1.1	Введение. Основные понятия.	Управление учетными записями пользователей и создание групп Упражнение
1.2	Стандарты и спецификации в области ИБ. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.	Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.
1.3	Категории и модели информационной безопасности	Управление разрешениями в файловой системе NTFS

		Упражнение
1.4	Идентификация и аутентификация пользователей. Понятие несанкционированного доступа.	. Управление локальными политиками безопасности Упражнение
2	**Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем**	
2.1	Программно-аппаратные средства шифрования.	Создание и изменение шаблона политики безопасности Упражнение
2.2	Защита компонентов ПЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.	Анализ шаблона политики безопасности Упражнение

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Основные принципы создания и применения программно-аппаратных средств обеспечения информационной безопасности.**	
1.1	Введение. Основные понятия.	Построение системы резервного копирования в ОС семейства WIndows Установка и настройка ПО VipNet
1.2	Стандарты и спецификации в области ИБ. Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.	Использование инструментальных средств анализа защищённости. Установка и использование сканера Nessus.
1.3	Категории и модели информационной безопасности	Обзор средств разграничения доступа на активном оборудовании
1.4	Идентификация и аутентификация пользователей. Понятие несанкционированного доступа.	Использование средств разграничения доступа на нескольких коммутаторах
2	**Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности, взаимодействие с общесистемными компонентами вычислительных систем**	
2.1	Программно-аппаратные средства шифрования.	Создание и удаление виртуальных сетей на коммутаторе Catalyst 2950
2.2	Защита компонентов ПЭВМ. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.	Использование инструментальных средств анализа защищённости. Установка и использование сканера Nessus.