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

Факультет ***Математики и информационных технологий***
Кафедра ***Прикладной информатики и программирования***

Аннотация рабочей программы дисциплины (модуля)

дисциплина ***Техническая защита информации***

Блок Б1, базовая часть, Б1.Б.28
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 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: 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
	2 этап: Умения	Обучающийся должен уметь: 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
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: навыками определения информационных ресурсов, подлежащих защите, угроз безопасности информации и возможных путей их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

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: особенности установки, настройки и обслуживания программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
	2 этап: Умения	Обучающийся должен уметь: выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: навыками выполнения работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

2. Место дисциплины (модуля) в структуре образовательной программы

Для освоения дисциплины студенты используют знания, умения и навыки, сформированные в процессе изучения дисциплин «Сети и системы передачи информации», «Администрирование информационных систем».
Цель освоения дисциплины настоящего курса является теоретическая и практическая подготовленность обучающегося к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и в защищаемых помещениях

Дисциплина изучается на 3 курсе в 5, 6 семестрах

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 7 зач. ед., 252 акад. ч.

Объем дисциплины	**Всего часов**
	Очная форма обучения
Общая трудоемкость дисциплины	252

Учебных часов на контактную работу с преподавателем:	
лекций	28
практических (семинарских)	44
лабораторных	24
другие формы контактной работы (ФКР)	1,4
Учебных часов на контроль (включая часы подготовки):	34,8
зачет	
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	119,8

Формы контроля	Семестры
зачет	5
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	**Модуль 1**	**8**	**12**	**0**	**40**
1.1	Характеристика государственной системы противодействия технической разведке	4	6	0	20
1.2	Свойства и виды информации	4	6	0	20
2	**Модуль 2**	**20**	**32**	**24**	**79,8**
2.1	Демаскирующие признаки объектов наблюдения и сигналов	4	8	6	20
2.2	Средства и методы технической разведки	4	8	6	20
2.3	Способы и средства перехвата сигналов	6	8	6	20
2.4	Технические каналы утечки информации. Оптические, электромагнитные радиоэлектронные, акустические и виброакустические каналы утечки информации каналы утечки информации	6	8	6	19,8
	Итого	**28**	**44**	**24**	**119,8**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Модуль 1**	
1.1	Характеристика государственной системы противодействия	Нормативные документы по противодействию технической разведке

	технической разведке	
1.2	Свойства и виды информации	Виды, источники и носители защищаемой информации.
2	**Модуль 2**	
2.1	Демаскирующие признаки объектов наблюдения и сигналов	Опасные сигналы и их источники
2.2	Средства и методы технической разведки	Классификация технической разведки, основные этапы и процедуры добывания информации технической разведкой.
2.3	Способы и средства перехвата сигналов	Способы и средства наблюдения. Способы и средства подслушивания. Способы прослушивания помещений. Дистанционные системы прослушивания. Способы и средства добывания информации о радиоактивных веществах. Специальные системы получения информации
2.4	Технические каналы утечки информации. Оптические, электромагнитные радиоэлектронные, акустические и виброакустические каналы утечки информации каналы утечки информации	Технические каналы утечки информации. Оптические, электромагнитные радиоэлектронные, акустические и виброакустические каналы утечки информации каналы утечки информации

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Модуль 1**	
1.1	Характеристика государственной системы противодействия технической разведке	Нормативные документы по противодействию технической разведке
1.2	Свойства и виды информации	Виды, источники и носители защищаемой информации.
2	**Модуль 2**	
2.1	Демаскирующие признаки объектов наблюдения и сигналов	Опасные сигналы и их источники
2.2	Средства и методы технической разведки	Классификация технической разведки, основные этапы и процедуры добывания информации технической разведкой.
2.3	Способы и средства перехвата сигналов	Способы и средства наблюдения. Способы и средства подслушивания. Способы прослушивания помещений. Дистанционные системы прослушивания. Способы и средства добывания информации о радиоактивных веществах. Специальные системы получения информации
2.4	Технические каналы утечки информации. Оптические, электромагнитные радиоэлектронные, акустические и виброакустические каналы утечки информации каналы утечки	Характеристики технических каналов утечки информации, физические принципы технических каналов передачи информации. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Электрические каналы утечки

	информации	информации. Материально-вещественные каналы утечки информации. Комплексное использование каналов утечки информации.

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
2	**Модуль 2**	
2.1	Демаскирующие признаки объектов наблюдения и сигналов	Опасные сигналы и их источники
2.2	Средства и методы технической разведки	Классификация технической разведки, основные этапы и процедуры добывания информации технической разведкой.
2.3	Способы и средства перехвата сигналов	Способы и средства наблюдения. Способы и средства подслушивания. Способы прослушивания помещений. Дистанционные системы прослушивания. Способы и средства добывания информации о радиоактивных веществах. Специальные системы получения информации
2.4	Технические каналы утечки информации. Оптические, электромагнитные радиоэлектронные, акустические и виброакустические каналы утечки информации каналы утечки информации	Характеристики технических каналов утечки информации, физические принципы технических каналов передачи информации. Оптические каналы утечки информации. Радиоэлектронные каналы утечки информации. Электрические каналы утечки информации. Материально-вещественные каналы утечки информации. Комплексное использование каналов утечки информации.