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 ***Информационная безопасность предприятия***

Блок Б1, базовая часть, Б1.Б.33
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 принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)

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 принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5)	1 этап: Знания	Обучающийся должен знать: особенности организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
	2 этап: Умения	Обучающийся должен уметь: принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть навыками принятия участия в организации и сопровождении аттестации объекта информатизации по требованиям безопасности 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».
Целью курса является формирование у студентов знания и умения по разработке защищенных автоматизированных систем предприятий, по использованию методов и средств защиты автоматизированных систем предприятий. Курс должен решить следующие задачи: 1) раскрыть основные вопросы теоретических основ защиты информационных процессов в автоматизированных системах предприятий; 2) ознакомить студентов с основными нормативными правовыми актами в области информационной безопасности и защиты информации на предприятиях; 3) дать представление о возможных угрозах и нарушителях информационной безопасности в автоматизированных системах предприятий.

Дисциплина изучается на 4 курсе в 8 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 2 зач. ед., 72 акад. ч.

Объем дисциплины	**Всего часов**
	Очная форма обучения

Общая трудоемкость дисциплины	72
Учебных часов на контактную работу с преподавателем:	
лекций	16
практических (семинарских)	
лабораторных	16
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	
зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	39,8

Формы контроля	**Семестры**
зачет	8

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**	**0**	**4**	**18**
1.1	Организационно-правовое обеспечение информационной безопасности предприятия	4	0	0	6
1.2	Информационные системы предприятий	0	0	4	6
1.3	Угрозы информации в автоматизированных системах предприятий	4	0	0	6
2	**Модуль 2**	**8**	**0**	**12**	**21,8**
2.1	Методы и модели оценки уязвимости информации в автоматизированных системах предприятий	4	0	0	6
2.2	Методы определения требований к защите информации на предприятиях.	0	0	4	6
2.3	Функции и задачи защиты информации на предприятиях.	4	0	4	6
2.4	Стратегии защиты информации на предприятиях.	0	0	4	3,8
	Итого	**16**	**0**	**16**	**39,8**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	**Наименование раздела / темы дисциплины**	**Содержание**

1	**Модуль 1**	
1.1	Организационно-правовое обеспечение информационной безопасности предприятия	Основные принципы засекречивания информации на предприятиях
1.3	Угрозы информации в автоматизированных системах предприятий	Классы каналов несанкционированного получения информации на предприятиях. Причины нарушения целостности информации на предприятиях. Виды угроз информационным системам предприятий. Виды потерь информации. Убытки, связанные с информационным обменом на предприятих
2	**Модуль 2**	
2.1	Методы и модели оценки уязвимости информации в автоматизированных системах предприятий	Эмпирический подход к оценке уязвимости информации на предприятиях. Практическая реализация модели «угроза – защита» на предприятии. Использование моделей оценки уязвимости информации на предприятиях.
2.3	Функции и задачи защиты информации на предприятиях.	Общие положения. Методы формирования функций защиты на предприятиях. Классы задач защиты информации на предприятиях. Функции защиты. Состояния и функции системы защиты информации на предприятиях

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Модуль 1**	
1.2	Информационные системы предприятий	Источники конфиденциальной информации в информационных системах предприятий. Виды технических средств информационных систем предприятий.
2	**Модуль 2**	
2.2	Методы определения требований к защите информации на предприятиях.	Требования к безопасности информационных систем на предприятиях. Классы защищенности средств вычислительной техники от несанкционированного доступа на предприятиях
2.3	Функции и задачи защиты информации на предприятиях.	Методы формирования функций защиты информации на предприятиях. Классы задач защиты информации на предприятиях. Функции защиты информации на предприятиях . Состояния и функции системы защиты информации на предприятиях
2.4	Стратегии защиты информации на предприятиях.	Способы и средства защиты информации на предприятиях. Криптографические методы защиты информации на предприятиях . Требования к криптосистемам на предприятиях.