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 автоматизированных систем***

Блок Б1, базовая часть, Б1.Б.32
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 применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)

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 применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2)	1 этап: Знания	Обучающийся должен знать: программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
	2 этап: Умения	Обучающийся должен уметь: применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть навыками применения программных средств системного, прикладного и специального назначения, инструментальных средств, языков и систем программирования для решения профессиональных задач
Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей	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 (ОПК-7)		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

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, по использованию методов и средств защиты автоматизированных систем. Курс должен решить следующие задачи: 1) раскрыть основные вопросы теоретических основ защиты информационных процессов в автоматизированных системах; 2) ознакомить студентов с основными нормативными правовыми актами в области информационной безопасности и защиты информации; 3) дать представление о возможных угрозах и нарушителях информационной безопасности в автоматизированных системах.

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 3 зач. ед., 108 акад. ч.

Объем дисциплины	Всего часов
	Очная форма обучения
Общая трудоемкость дисциплины	108
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
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	24

Формы контроля	Семестры
экзамен	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**	**4**	**10**	**6**	**12**
1.1	Организационно-правовое обеспечение информационной безопасности в автоматизированных системах	0	4	0	2
1.2	Информация как объект юридической защиты.	0	2	0	4
1.3	Информационные системы	2	2	0	4
1.4	Угрозы информации в автоматизированных системах	2	2	6	2
2	**Модуль 2**	**8**	**8**	**12**	**12**
2.1	Методы и модели оценки уязвимости информации в автоматизированных системах	2	2	0	4
2.2	Методы определения требований к защите информации.	2	2	0	4
2.3	Функции и задачи защиты информации.	2	2	6	2
2.4	Стратегии защиты информации.	2	2	6	2
	Итого	**12**	**18**	**18**	**24**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела /	Содержание

	темы дисциплины	
1	**Модуль 1**	
1.3	Информационные системы	Информация как продукт. Информационные услуги. Источники конфиденциальной информации в информационных системах. Виды технических средств информационных систем.
1.4	Угрозы информации в автоматизированных системах	Классы каналов несанкционированного получения информации. Причины нарушения целостности информации. Виды угроз информационным системам. Виды потерь информации. Убытки, связанные с информационным обменом
2	**Модуль 2**	
2.1	Методы и модели оценки уязвимости информации в автоматизированных системах	Эмпирический подход к оценке уязвимости информации. Система с полным перекрытием. Практическая реализация модели «угроза – защита». Использование моделей оценки уязвимости информации.
2.2	Методы определения требований к защите информации.	Анализ существующих методик определения требований к защите информации. Требования к безопасности информационных систем в России. Классы защищенности средств вычислительной техники от несанкционированного доступа. Критерии оценки безопасности информационных технологий
2.3	Функции и задачи защиты информации.	Общие положения. Методы формирования функций защиты. Классы задач защиты информации. Функции защиты. Состояния и функции системы защиты информации
2.4	Стратегии защиты информации.	Способы и средства защиты информации. Криптографические методы защиты информации. Требования к криптосистемам. Основные алгоритмы шифрования

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Модуль 1**	
1.1	Организационно-правовое обеспечение информационной безопасности в автоматизированных системах	Основные принципы засекречивания информации.
1.2	Информация как объект юридической защиты.	Государственная система правового обеспечения защиты информации в Российской Федерации.
1.3	Информационные системы	Источники конфиденциальной информации в информационных системах. Виды технических средств информационных систем.
1.4	Угрозы информации в автоматизированных системах	Причины нарушения целостности информации. Виды угроз информационным системам. Виды потерь информации
2	**Модуль 2**	
2.1	Методы и модели оценки уязвимости информации в	Система с полным перекрытием. Практическая реализация модели «угроза – защита».

	автоматизированных системах	
2.2	Методы определения требований к защите информации.	Требования к безопасности информационных систем в России. Классы защищенности средств вычислительной техники от несанкционированного доступа
2.3	Функции и задачи защиты информации.	Методы формирования функций защиты. Классы задач защиты информации. Функции защиты.
2.4	Стратегии защиты информации.	Криптографические методы защиты информации. Основные алгоритмы шифрования

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Модуль 1**	
1.4	Угрозы информации в автоматизированных системах	Классы каналов несанкционированного получения информации. Причины нарушения целостности информации. Виды угроз информационным системам. Виды потерь информации. Убытки, связанные с информационным обменом
2	**Модуль 2**	
2.3	Функции и задачи защиты информации.	Методы формирования функций защиты. Классы задач защиты информации. Функции защиты. Состояния и функции системы защиты информации
2.4	Стратегии защиты информации.	Способы и средства защиты информации. Криптографические методы защиты информации. Требования к криптосистемам. Основные алгоритмы шифрования