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 ***Модели безопасности компьютерных систем***

Блок Б1, вариативная часть, Б1.В.ДВ.05.02
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 осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)
Способен участвовать в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах (ПСК1-1)

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)
Способен участвовать в разработке формальных моделей политик безопасности, политик управления доступом и информационными потоками в компьютерных системах (ПСК1-1)	1 этап: Знания	Обучающийся должен знать: принципы организации процесса аудита информационной безопасности и подготовки отчетных документов по его результатам
	2 этап: Умения	Обучающийся должен уметь: составлять программу аудита информационной безопасности, определять его область действия и критерии
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: практическими приемами проведения аудита информационной безопасности, методами сбора данных
Способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9)	1 этап: Знания	Обучающийся должен знать:подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности;
	2 этап: Умения	Обучающийся должен уметь: осуществлять подбор, изучение и обобщение научнотехнической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной

		безопасности по профилю своей профессиональной деятельности;
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Модели безопасности компьютерных систем» относится к числу дисциплин вариативной части профессионального цикла.

Целью изучения дисциплины «Модели безопасности компьютерных систем» является обучение специалистов принципам формального моделирования и анализа безопасности компьютерных систем (КС), реализующих управление доступом и информационными потоками, а также содействие фундаментализации образования, формированию научного мировоззрения и развитию системного мышления.

Для ее успешного изучения необходимы знания и умения, приобретенные в результате освоения курсов «Техническая защита информации», «Технологии и методы программирования», «Математическая логика и теория алгоритмов», «Основы информационной безопасности», «Программно-аппаратные средства защиты информации», а также некоторых разделов дисциплин «Информационные технологии» и «ТСети и системы передачи информации». Кроме того, необходимо наличие практических навыков программирования на одном из языков программирования высокого уровня.

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)	0,2
Учебных часов на контроль (включая часы подготовки):	
зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	59,8

Формы контроля	Семестры
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	**Раздел 1:**	**4**	**4**	**4**	**10**
1.1	Введение в теоретический подход к обеспечению информационной безопасности.	1	0	0	2
1.2	Математические основы построения моделей безопасности.	1	2	2	4
1.3	Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU).	2	2	2	4
2	**Раздел 2:**	**8**	**14**	**14**	**49,8**
2.1	Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД).	2	2	2	12
2.2	Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа Take-Grant.	2	4	4	12
2.3	Модели компьютерных систем с мандатным управлением.Белла-ЛаПадулы. Модель	2	4	2	8
2.4	Модели компьютерных систем с ролевым управлением доступом	2	2	4	8
2.5	Развитие формальных моделей	0	2	2	9,8

	безопасности компьютерных систем.				
	Итого	**12**	**18**	**18**	**59,8**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Раздел 1:**	
1.2	Математические основы построения моделей безопасности.	
1.3	Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU).	
2	**Раздел 2:**	
2.1	Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД).	
2.2	Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа Take-Grant.	
2.3	Модели компьютерных систем с мандатным управлением.Белла-ЛаПадулы. Модель	
2.4	Модели компьютерных систем с ролевым управлением доступом	
2.5	Развитие формальных моделей безопасности компьютерных систем.	

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Раздел 1:**	
1.2	Математические основы построения моделей безопасности.	
1.3	Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU).	
2	**Раздел 2:**	
2.1	Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД).	
2.2	Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа Take-Grant.	
2.3	Модели компьютерных систем с мандатным управлением.Белла-ЛаПадулы. Модель	
2.4	Модели компьютерных систем с ролевым управлением доступом	
2.5	Развитие формальных моделей безопасности компьютерных систем.	

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Раздел 1:**	
1.1	Введение в теоретический подход к обеспечению информационной безопасности.	
1.2	Математические основы построения моделей безопасности.	
1.3	Модели компьютерных систем с дискреционным управлением. Модель матрицы доступов Харрисона-Руззо-Ульмана (HRU).	
2	**Раздел 2:**	
2.1	Модели компьютерных систем с дискреционным управлением. Модель типизированной матрицы доступов (ТМД).	
2.2	Модели компьютерных систем с дискреционным управлением. Модель распространения прав доступа Take-Grant.	
2.3	Модели компьютерных систем с мандатным управлением.Белла-	

	ЛаПадулы. Модель	
2.4	Модели компьютерных систем с ролевым управлением доступом	