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 ***Б1.В.ДВ.01.02 Основы информационной безопасности***

часть, формируемая участниками образовательных отношений

Направление

02.03.03 ***Математическое обеспечение и администрирование информационных систем***

код наименование направления

Программа

Сетевое программирование и администрирование информационных систем

Форма обучения

Очная

Для поступивших на обучение в
2023 г.

Стерлитамак 2023

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)
ПК-2. Способен использовать знания направлений развития компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств; операционных систем; операционных и сетевых оболочек, сервисных программ; тенденции развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности	ПК-2.1. Знает направления развития компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств; операционных систем, операционных и сетевых оболочек, сервисных программ; тенденции развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности.	Обучающийся должен: Знать направления развития компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств; операционных систем, операционных и сетевых оболочек, сервисных программ; тенденции развития функций и архитектур проблемно ориентированных программных систем и комплексов в профессиональной деятельности.
	ПК-2.2. Умеет программировать для компьютеров с различной современной архитектурой.	Обучающийся должен: Уметь программировать для компьютеров с различной современной архитектурой.
	ПК-2.3. Имеет практический опыт выбора архитектуры и комплексирования современных компьютеров, систем, комплексов и сетей системного администрирования.	Обучающийся должен: Иметь практический опыт выбора архитектуры и комплексирования современных компьютеров, систем, комплексов и сетей системного администрирования.

2. Цели и место дисциплины (модуля) в структуре образовательной программы

Цели изучения дисциплины:
Дисциплина «Основы информационной безопасности» входит в общепрофессиональный цикл, является дисциплиной, дающей начальные представления и понятия в области информационной безопасности, определяющей потребности в развитии интереса к изучению учебных дисциплин и профессиональных модулей, способности к личному

самоопределению и самореализации в учебной деятельности.
Основной задачей преподавания дисциплины является подготовка специалистов, обладающих знаниями, навыками, умениями в сфере обеспечения информационной безопасности организаций различных форм собственности.
Уровень освоения содержания дисциплины предполагает: - Знакомство с основными понятиями информационной безопасности, информационными угрозами, их классификацией, и возможными последствиями для организаций различных форм собственности; Уяснение вопросов обеспечения информационной безопасности организации и проблем создания (концептуального проектирования) систем информационной безопасности; - Принятие обоснованных решений по выбору политики информационной безопасности (ИБ) и оценки эффективности инвестиций в ИБ
Знания, навыки и умения, приобретенные в процессе изучения дисциплины в ходе лекций, практических занятий и самостоятельной работы, должны всесторонне использоваться студентами в процессе дальнейшей профессиональной деятельности при решении широкого класса аналитических задач финансово-экономического характера.

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	16
практических (семинарских)	16
лабораторных	16
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	**Теоретические основы информационной безопасности**	**8**	**8**	**8**	**32**
1.1	Основные понятия теории информационной безопасности	2	2	2	6
1.2	Информация как объект защиты	2	2	2	10
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	2	2	2	10
1.4	Угрозы информационной безопасности	2	2	2	6
2	**Методология защиты информации**	**8**	**8**	**8**	**27,8**
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	2	2	2	6
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	2	2	2	6
2.3	Политика и модели безопасности	2	2	2	10
2.4	Обзор международных стандартов информационной безопасности	2	2	2	5,8
	Итого	**16**	**16**	**16**	**59,8**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Теоретические основы информационной безопасности**	
1.1	Основные понятия теории информационной безопасности	История становления и предметная область теории информационной безопасности. Систематизация понятий в области защиты информации. Основные термины и определения правовых понятий в области информационных отношений и защиты информации. Понятия предметной области «Защита информации». Основные принципы построения систем защиты. Концепция комплексной защиты информации. Задачи защиты информации.
1.2	Информация как объект защиты	Понятие об информации как объекте защиты. Уровни представления информации. Основные свойства защищаемой информации. Виды и формы представления информации. Информационные ресурсы. Структура и шкала ценности информации. Классификация информационных ресурсов. Правовой режим информационных ресурсов.
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	Информационная безопасность и ее место в системе национальной безопасности Российской Федерации. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность.
1.4	Угрозы информационной	Анализ уязвимостей системы. Классификация

	безопасности	угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.
2	**Методология защиты информации**	
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	Определение и основные способы несанкционированного доступа. Методы защиты от НСД. Организационные методы защиты от НСД. Инженерно-технические методы защиты от НСД. Построение систем защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация. Основные направления и цели использования криптографических методов. Защита от угрозы нарушения конфиденциальности на уровне содержания информации.
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	Защита целостности информации при хранении. Защита целостности информации при обработке. Защита целостности информации при транспортировке. Защита от угрозы нарушения целостности информации на уровне содержания. Построение систем защиты от угрозы отказа доступа к информации. Защита семантического анализа и актуальности информации.
2.3	Политика и модели безопасности	Политика безопасности. Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности. Политика и модели дискреционного доступа. Парольные системы разграничения доступа. Политика и модели мандатного доступа. Теоретико-информационные модели. Политика и модели тематического разграничения доступа. Ролевая модель безопасности.
2.4	Обзор международных стандартов информационной безопасности	Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности информационных технологий США. Единые критерии безопасности информационных технологий.

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Теоретические основы информационной безопасности**	
1.1	Основные понятия теории информационной безопасности	Обзор защищаемых объектов и систем.
1.2	Информация как объект защиты	Определение объектов защиты на типовом объекте информатизации.
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	Классификация защищаемой информации по видам тайны и степеням конфиденциальности.

1.4	Угрозы информационной безопасности	Определение угроз объекта информатизации и их классификация.
2	**Методология защиты информации**	
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.
2.3	Политика и модели безопасности	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.
2.4	Обзор международных стандартов информационной безопасности	Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности.

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Теоретические основы информационной безопасности**	
1.1	Основные понятия теории информационной безопасности	Систематизация понятий в области защиты информации. Основные термины и определения понятий в области информационной защиты информации. Принципы построения систем защиты. Задачи защиты информации. Средства реализации комплексной защиты информации.
1.2	Информация как объект защиты	Уровни представления информации. Виды и формы представления информации. Свойства защищаемой информации. Структура и шкала ценности информации. Классификация информационных ресурсов.
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	Роль и место информационной безопасность в системе национальной безопасности РФ. Нормативная деятельность, функции и задачи органов обеспечения информационной безопасности и защиты информации.
1.4	Угрозы информационной безопасности	Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.
2	**Методология защиты информации**	
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	Методы защиты от несанкционированного доступа. Организационные и инженерно-технические методы защиты от несанкционированного доступа. Построение систем защиты от угрозы утечки по техническим

		каналам. Криптографические методы защиты. Защита от угрозы нарушения конфиденциальности информации.
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	Защита целостности информации при хранении, обработке, транспортировке. Построение систем защиты от угрозы отказа доступа к информации. Семантический анализ.
2.3	Политика и модели безопасности	Модели разграничения доступа в рамках политики безопасности. Модели дискреционного доступа. Парольные системы разграничения доступа. Модели тематического разграничения доступа.
2.4	Обзор международных стандартов информационной безопасности	Роль стандартов информационной безопасности. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга), TCSEC. Европейские критерии безопасности информационных технологий (ITSEC). Федеральные критерии безопасности информационных технологий США. Единые критерии безопасности информационных технологий. Группа международных стандартов 270000.