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.О.23 Информационная безопасность***

обязательная часть

Направление

44.03.05 ***Педагогическое образование (с двумя профилями подготовки)***
код наименование направления

Программа

Физическая культура, Безопасность жизнедеятельности

Форма обучения

Заочная

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)
ОПК-2. Способен участвовать в разработке основных и дополнительных образовательных программ, разрабатывать отдельные их компоненты (в том числе с использованием информационно-коммуникационных технологий)	ОПК-2.1. Показывает пути достижения образовательных результатов в области ИКТ	Обучающийся должен: знать принципы построения и функционирования образовательных систем; закономерности организации образовательного процесса; специфику использования ИКТ в педагогической деятельности с учетом информационной безопасности.
	ОПК-2.2. Способен разрабатывать и применять отдельные компоненты основных и дополнительных образовательных программ в реальной и виртуальной образовательной среде	Обучающийся должен: уметь разрабатывать и отдельные компоненты основных и дополнительных образовательных программ в реальной и виртуальной образовательной среде с учетом информационной безопасности, в том числе с использованием ИКТ.
	ОПК-2.3. Способен осуществлять поиск информации с применением современных технологий	Обучающийся должен: владеть технологиями безопасного поиска, хранения и обработки информации для реализации основных и дополнительных образовательных программ с использованием ИКТ.
ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-9.1. Знать и понимать принципы работы современных информационных технологий	Обучающийся должен: знать принципы работы современных информационных технологий с учетом информационной безопасности
	ОПК-9.2. Уметь использовать принципы работы современных информационных	Обучающийся должен: уметь использовать современные информационные технологии с учетом информационной

	технологий для решения задач профессиональной деятельности	безопасности.
	ОПК-9.3. Владеть навыками использования современных информационных технологий для решения задач профессиональной деятельности	Обучающийся должен: владеть навыками использования современных информационных технологий для решения задач профессиональной деятельности с учетом информационной безопасности

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

Цели изучения дисциплины:
Дисциплина «Информационная безопасность» 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 5 курсе в 9, 10 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 216 акад. ч.

Объем дисциплины	**Всего часов**
	Заочная форма обучения
Общая трудоемкость дисциплины	216
Учебных часов на контактную работу с преподавателем:	
лекций	8

практических (семинарских)	14
другие формы контактной работы (ФКР)	1,2
Учебных часов на контроль (включая часы подготовки):	7,8
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	185

Формы контроля	Семестры
экзамен	10

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**	**4**	**6**	**0**	**95**
1.1	Основные понятия теории информационной безопасности	2	2	0	20
1.2	Информация как объект защиты	0	2	0	25
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	0	0	0	25
1.4	Угрозы информационной безопасности	2	2	0	25
2	**Методология защиты информации**	**4**	**8**	**0**	**90**
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	2	2	0	22
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	2	2	0	23
2.3	Политика и модели безопасности	0	2	0	25
2.4	Обзор международных стандартов информационной безопасности	0	2	0	20
	Итого	**8**	**14**	**0**	**185**

4.2. Содержание дисциплины, структурированное по разделам (темам)

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.
1.4	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.

Курс лекционных занятий

№	Наименование раздела /	Содержание

	темы дисциплины	
1	**Теоретические основы информационной безопасности**	
1.1	Основные понятия теории информационной безопасности	История становления и предметная информационной безопасности 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.
1.4	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	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.