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.26 Основы информационной безопасности***

обязательная часть

Направление

01.03.02 ***Прикладная математика и информатика***
код наименование направления

Программа

Искусственный интеллект и анализ данных

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)
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Реализует нормы права при решении задач в рамках поставленной цели	Обучающийся должен: знать правовые нормы и методологические основы принятия управленческого решения
	УК-2.2. Умеет проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности	Обучающийся должен: уметь анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ.
	УК-2.3. Владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно правовой документацией	Обучающийся должен: владеть методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.
ОПК-4. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-4.1. знать и понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства при решении задач профессиональной деятельности	Обучающийся должен: знать способы получения на основе информационных технологий новых знаний для решения профессиональных задач с учетом требований информационной безопасности и причин нарушения безопасности компьютерных систем.
	ОПК-4.2. уметь выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	Обучающийся должен: уметь применять информационные технологии и программные средства, в том числе отечественного производства, для анализа и оценивания эффективности средств защиты информации;

		ориентироваться в современных и перспективных методах защиты информации.
	ОПК-4.3. иметь практический опыт применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	Обучающийся должен: владеть навыками применения методов защиты информации в компьютерных системах; иметь практический опыт применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности

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

Цели изучения дисциплины:
Дисциплина «Основы информационной безопасности» 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**	**30**
1.1	Основные понятия и задачи информационной безопасности	4	4	4	10
1.2	Основы защиты информации	2	2	2	10
1.3	Угрозы безопасности защищаемой информации.	2	2	2	10
2	**Методология защиты информации**	**8**	**8**	**8**	**29,8**
2.1	Методологические подходы к защите информации	4	2	2	10
2.2	Нормативно правовое регулирование защиты информации	2	2	4	10
2.3	Защита информации в автоматизированных (информационных) системах	2	4	2	9,8
	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 и задачи информационной безопасности	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от не информированности в области информационной безопасности.
1.2	Основы защиты информации	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации.Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.
1.3	Угрозы безопасности защищаемой информации.	Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к информации. Уязвимости. Методы оценки уязвимости информации.
2	**Методология защиты информации**	
2.1	Методологические подходы к защите информации	Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации.
2.2	Нормативно правовое регулирование защиты информации	Организационная структура системы защиты информации. Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации.
2.3	Защита информации в автоматизированных (информационных) системах	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. Программные и программно-аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутри

		объектовый режим. Принципы построения организационно-распорядительной системы.

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Теоретические основы информационной безопасности**	
1.1	Основные понятия и задачи информационной безопасности	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от не информированности в области информационной безопасности.
1.2	Основы защиты информации	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации.Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.
1.3	Угрозы безопасности защищаемой информации.	Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к информации. Уязвимости. Методы оценки уязвимости информации.
2	**Методология защиты информации**	
2.1	Методологические подходы к защите информации	Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации.
2.2	Нормативно правовое регулирование защиты информации	Организационная структура системы защиты информации. Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации.
2.3	Защита информации в автоматизированных (информационных)	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных)

	системах	системах. Программные и программно-аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутри объектовый режим. Принципы построения организационно-распорядительной системы.

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Теоретические основы информационной безопасности**	
1.1	Основные понятия и задачи информационной безопасности	Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем. Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от не информированности в области информационной безопасности.
1.2	Основы защиты информации	Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи. Цели и задачи защиты информации. Основные понятия в области защиты информации.Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.
1.3	Угрозы безопасности защищаемой информации.	Понятие угрозы безопасности информации. Системная классификация угроз безопасности информации. Каналы и методы несанкционированного доступа к информации. Уязвимости. Методы оценки уязвимости информации.
2	**Методология защиты информации**	
2.1	Методологические подходы к защите информации	Анализ существующих методик определения требований к защите информации. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации. Виды мер и основные принципы защиты информации.
2.2	Нормативно правовое регулирование защиты информации	Организационная структура системы защиты информации. Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и

		документы системы сертификации РФ в области защиты информации.
2.3	Защита информации в автоматизированных (информационных) системах	Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. Программные и программно-аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутри объектовый режим. Принципы построения организационно-распорядительной системы.