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.11 Информационная безопасность***

обязательная часть

Направление

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

Программа

Программирование и дизайн виртуальной и дополненной реальности

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)
ОПК-4. Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	ОПК-4.1. Основные методы получения новых знаний с помощью информационных технологий для решения задач в области профессиональной деятельности с учетом требований информационной безопасности; - стандарты оформления программной документации и причины нарушения компьютерной безопасности.	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. Применять информационные технологии в практической деятельности и анализировать полученные решения вычислительных задач; - на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств защиты информации; ориентироваться в современных и перспективных математических методах защиты информации.	Обучающийся должен: уметь применять информационные технологии для анализа и оценивания эффективности средств защиты информации; ориентироваться в современных и перспективных методах защиты информации.
	ОПК-4.3. Владение информационными технологиями как средством получения новых знаний; методами информационной и кадровой безопасности в коммуникационной деятельности.	Обучающийся должен: владеть навыками применения методов защиты информации в компьютерных системах; методами информационной и кадровой безопасности в коммуникационной деятельности.

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, лабораторных занятий и самостоятельной работы, должны всесторонне использоваться студентами в процессе дальнейшей профессиональной деятельности.
В структуре образовательной программы дисциплина находится в обязательной части.

Дисциплина изучается на 2 курсе в 4 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 2 зач. ед., 72 акад. ч.

Объем дисциплины	**Всего часов**
	Очная форма обучения
Общая трудоемкость дисциплины	72
Учебных часов на контактную работу с преподавателем:	
лекций	6
практических (семинарских)	
лабораторных	12
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	
зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	53,8

Формы контроля	**Семестры**
зачет	4

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**	**0**	**4**	**24**
1.1	Основные понятия теории информационной безопасности	2	0	2	6
1.2	Информация как объект защиты	0	0	0	6
1.3	Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности	0	0	0	6
1.4	Угрозы информационной безопасности	2	0	2	6
2	**Методология защиты информации**	**2**	**0**	**8**	**29,8**
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	2	0	2	8
2.2	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа	0	0	2	8
2.3	Политика и модели безопасности	0	0	4	8
2.4	Обзор международных стандартов информационной безопасности	0	0	0	5,8
	Итого	**6**	**0**	**12**	**53,8**

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	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.
1.4	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.

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Теоретические основы информационной безопасности**	
1.1	Основные понятия теории информационной безопасности	Построения систем защиты. Задачи защиты информации. Средства реализации комплексной защиты информации.
1.4	Угрозы информационной безопасности	Неформальная модель нарушителя. Оценка уязвимости системы. Основные направления и методы реализации угроз.
2	**Методология защиты информации**	
2.1	Построение систем защиты от угрозы нарушения конфиденциальности	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	. Построение систем защиты от угрозы отказа доступа к информации. Семантический анализ. Защита целостности информации при хранении, обработке, транспортировке
2.3	Политика и модели безопасности	Модели разграничения доступа в рамках политики безопасности. Модели дискреционного доступа. Парольные системы разграничения доступа. Модели тематического разграничения доступа.