Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 30.10.2023 11:13:22
Уникальный программный ключ:
b683afe664d7e9f64175886cf9626a198149ad36

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.17 Методы и средства защиты информации***

обязательная часть

Направление

09.03.03 ***Прикладная информатика***
код наименование направления

Программа

Мобильные и сетевые технологии

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 понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности;	ОПК-2.1. Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.	Обучающийся должен: знать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.
	ОПК-2.2. Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.	Обучающийся должен: уметь выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности.
	ОПК-2.3. Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.	Обучающийся должен: владеть навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности.
ОПК-4. Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;	ОПК-4.1. Знает основные стандарты оформления технической документации на раз-личных стадиях жизненного цикла информационной системы.	Обучающийся должен: знать основные стандарты оформления технической документации на раз-личных стадиях жизненного цикла информационной системы.
	ОПК-4.2. Умеет применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.	Обучающийся должен: уметь применять стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы.

	ОПК-4.3. Владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.	Обучающийся должен: владеет навыками составления технической документации на различных этапах жизненного цикла информационной системы.
ОПК-5. Способен инсталлировать программное и аппаратное обеспечение для информационных и автоматизированных систем;	ОПК-5.1. Знает основы системного администрирования, администрирования СУБД, современные стандарты информационного взаимодействия систем.	Обучающийся должен: знать основы системного администрирования, администрирования СУБД, современные стандарты информационного взаимодействия систем.
	ОПК-5.2. Умеет выполнять параметрическую настройку информационных и автоматизированных систем	Обучающийся должен: уметь выполнять параметрическую настройку информационных и автоматизированных систем
	ОПК-5.3. Владеет навыками инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем	Обучающийся должен: владеть навыками инсталляции программного и аппаратного обеспечения информационных и автоматизированных систем

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

Цели изучения дисциплины:
Дисциплина «Методы и средства защиты информации» 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 реализуется в рамках части, формируемой участниками образовательных отношений .

Дисциплина изучается на 4 курсе в 7, 8 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 180 акад. ч.

Объем дисциплины	**Всего часов**
	Заочная форма обучения
Общая трудоемкость дисциплины	180
Учебных часов на контактную работу с преподавателем:	
лекций	6
практических (семинарских)	12
лабораторных	12
другие формы контактной работы (ФКР)	1,2
Учебных часов на контроль (включая часы подготовки):	7,8
экзамен	
Учебных часов на самостоятельную работу обучающихся (СР)	141

Формы контроля	**Семестры**
экзамен	8

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	**Криптография донаучного периода.**	**1**	**2**	**1**	**40**
1.1	Донаучный период криптографии.	0	1	1	30
1.2	Основные криптографические примитивы.	1	1	0	10
2	**Алгоритмы симметричного шифрования.**	**2**	**7**	**6**	**50**
2.1	Требования к алгоритмам симметричного шифрования.	1	0	0	16

	Режимы выполнения.				
2.2	Алгоритмы симметричного шифрования ГОСТ и DES.	1	7	6	34
3	**Алгоритмы асимметричного шифрования.**	**3**	**3**	**5**	**51**
3.1	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	1	1	2	20
3.2	Хэш-функции.	1	1	1	15
3.3	Электронная цифровая подпись.	1	1	2	16
	Итого	**6**	**12**	**12**	**141**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Криптография донаучного периода.**	
1.2	Основные криптографические примитивы.	Подстановки. Перестановки. Гаммирование. Нелинейное преобразование с помощью S-боксов. Комбинированные методы.
2	**Алгоритмы симметричного шифрования.**	
2.1	Требования к алгоритмам симметричного шифрования. Режимы выполнения.	Криптография. Сеть Фейштеля. Криптоанализ. Используемые критерии при разработке алгоритмов симметричного шифрования. 4 режима выполнения.
2.2	Алгоритмы симметричного шифрования ГОСТ и DES.	Алгоритм DES. Алгоритм генерации ключей. Алгоритм ГОСТ 2814. Сравнительный анализ ГОСТ и DES. Создание случайных чисел.
3	**Алгоритмы асимметричного шифрования.**	
3.1	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	Основные требования к алгоритмам ассиметричного шифрования. Математический аппарат алгоритма RSA.
3.2	Хэш-функции.	Требования к хэш-функциям. Простые хэш-функции. Сильные хэш- функции
3.3	Электронная цифровая подпись.	Требования к цифровой подписи. Прямая и арбитражная цифровые подписи.

Курс лабораторных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Криптография донаучного периода.**	
1.1	Донаучный период криптографии.	Программирование алгоритма Гронсфельда.
2	**Алгоритмы симметричного шифрования.**	
2.2	Алгоритмы симметричного шифрования ГОСТ и DES.	Разработка приложения алгоритма ГОСТ (шифрование/дешифрование).
3	**Алгоритмы асимметричного шифрования.**	
3.1	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	Программирование алгоритма RSA.
3.2	Хэш-функции.	Создание хеш-образа сообщения с помощью хеш-функции цепочки зашифрованных блоков.

3.3	Электронная цифровая подпись.	Создание электронной цифровой подписи на основе RSA.

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Криптография донаучного периода.**	
1.1	Донаучный период криптографии.	Разбор алгоритмов шифрования Цезаря, Гронефельда, Трипемиуса, Бодо. Шифрование биграммами.
1.2	Основные криптографические примитивы.	Частотные характеристики открытых сообщений. Определение частотных характеристик криптограммы. Определение вероятностных характеристик алфавита.
2	**Алгоритмы симметричного шифрования.**	
2.2	Алгоритмы симметричного шифрования ГОСТ и DES.	Работа с S-box, кодовой таблицей. Выполнение алгоритма ГОСТ (2 раунда). Дешифрование ГОСТ. Разработка соответствующих процедур.
3	**Алгоритмы асимметричного шифрования.**	
3.1	Требования к алгоритмам асимметрического шифрования Алгоритм RSA.	Генерация открытого и закрытого ключей RSA. Шифрование и дешифрование.
3.2	Хэш-функции.	Изучение сильных хэш-функций MD4, MD5.
3.3	Электронная цифровая подпись.	Изучение стандарта цифровой подписи DSS и ГОСТ 3410.