

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 22.08.2025 10:52:13
Уникальный программный ключ:
b683afe664d7e9f64175886cf9626a198149ad36

СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет Математики и информационных технологий
Кафедра Прикладной информатики и программирования

Аннотация рабочей программы дисциплины (модуля)

дисциплина ***Криптографические методы защиты информации***

Блок Б1, базовая часть, Б1.Б.30

цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

10.03.01

Информационная безопасность

код

наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очная

Для поступивших на обучение в
2020 г.

1. Перечень планируемых результатов обучения по дисциплине (модулю)

1.1. Перечень планируемых результатов освоения образовательной программы

Выпускник, освоивший программу высшего образования, в рамках изучаемой дисциплины, должен обладать компетенциями, соответствующими видам профессиональной деятельности, на которые ориентирована программа:

Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)

Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Формируемая компетенция (с указанием кода)	Этапы формирования компетенции	Планируемые результаты обучения по дисциплине (модулю)
Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)	1 этап: Знания	Обучающийся должен знать: понятие составляющие и проблемы информационной безопасности; объекты информатизации, включая компьютерные, автоматизированные, телекоммуникационные и аппаратные средства нормативно-правовые, экономические и технологические методы обеспечения информационной безопасности.
	2 этап: Умения	Обучающийся должен уметь: обосновать и сформулировать решения по применению технологических и нормативно-правовых средств и методов обеспечения информационной безопасности; применять криптографические и информационно-аналитические системы, информационные ресурсы и информационные технологии; сформулировать основные криптографические методы и методы стеганографии.
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: методом дискретного логарифмирования в конечных циклических группах; методом применения основных

		криптосистем и систем стенографирования; методом применения алгоритмов проверки чисел и многочленов на простоту, построения больших простых чисел, разложения чисел и многочленов на множители, дискретного логарифмирования в конечных циклических группах.
Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)	1 этап: Знания	Обучающийся должен знать: источники угроз безопасности информации, методы оценки уязвимости информации; методы пресечения разглашения конфиденциальной информации.
	2 этап: Умения	Обучающийся должен уметь: отыскивать необходимые нормативные правовые акты и информационные правовые нормы в системе действующего законодательства; применять действующую законодательную базу в области обеспечения информационной безопасности и защиты информации.
	3 этап: Владения (навыки / опыт деятельности)	Обучающийся должен владеть: навыками сопровождения и управления системами защиты информации.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина реализуется в рамках базовой части.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «Информатика и программирование», «Архитектура компьютера», «Алгебра», «Теория вероятностей и математическая статистика».

Дисциплина изучается на 3 курсе в 6 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	12
практических (семинарских)	18
лабораторных	18
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	
дифференцированный зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	59,8

Формы контроля	Семестры
дифференцированный зачет	6

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.	3	2	4	19,8
1.1	Донаучный период криптографии.	1	1	4	15
1.2	Основные криптографические примитивы.	2	1	0	4,8
2	Алгоритмы симметричного шифрования.	4	10	6	24
2.1	Требования к алгоритмам симметричного шифрования. Режимы выполнения.	2	0	0	7
2.2	Алгоритмы симметричного шифрования ГОСТ и DES.	2	10	6	17
3	Алгоритмы асимметричного шифрования.	5	6	8	16
3.1	Требования к алгоритмам асимметричного шифрования Алгоритм RSA.	2	2	4	7
3.2	Хэш-функции.	2	2	2	5
3.3	Электронная цифровая подпись.	1	2	2	4
	Итого	12	18	18	59,8

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Криптография донаучного периода.	
1.1	Донаучный период	Алгоритмы шифрования письма донаучного

	криптографии.	периода. Первые шифровальные машины.
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 асимметричного шифрования Алгоритм RSA.	Основные требования к алгоритмам асимметричного 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 асимметричного 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, Гронсфельда, Трипемуса, Бодо. Шифрование биграммami.
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	Работа с S-box, кодовой таблицей. Выполнение

	шифрования ГОСТ и DES.	алгоритма ГОСТ (2 раунда). Дешифрование ГОСТ. Разработка соответствующих процедур.
3	Алгоритмы асимметричного шифрования.	
3.1	Требования к алгоритмам асимметричного 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.