МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования

**«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Кафедра вычислительной техники и защиты информации

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ

УЧЕБНОЙ ДИСЦИПЛИНЫ

«КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ»

Уровень подготовки: высшее образование – бакалавриат

Направление подготовки
10.03.01 Информационная безопасность
(код и наименование направления подготовки)

Направленность подготовки (профиль)
Безопасность автоматизированных систем
(наименование профиля подготовки)

Квалификация (степень) выпускника
бакалавр

Форма обучения
очная

Год начала подготовки – 2015

Уфа 2016

Место дисциплины в структуре образовательной программы

Дисциплина «Криптографические методы защиты информации» является дисциплиной базовой части основной профессиональной образовательной программы (ОПОП).

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090900 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации 28 октября 2009 г. № 496, а также в соответствии с Приказом Министерства образования и науки Российской Федерации от 19 декабря 2013 г. N 1367 г. «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры» и актуализирована в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства образования и науки Российской Федерации 01 декабря 2016 г. № 1515. Является неотъемлемой частью основной профессиональной образовательной программы.

Цель освоения дисциплины – ознакомление с основополагающими принципами защиты информации с помощью криптографических методов и примерами реализации этих методов на практике.

Задачи дисциплины «Криптографические методы защиты информации» - дать основы:

- системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами, на основе применения криптографических методов;
- принципов разработки шифров;
- математических методов, используемых в криптографии.

Перечень результатов обучения

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций.

Планируемые результаты обучения по дисциплине

№	Формируемые компетенции	Код	Знать	Уметь	Владеть
1	Способность применять соответствующий математический аппарат для решения профессиональных задач	ОПК-2	основные теоремы, методы и алгоритмы построения классических систем криптографической защиты информации	применять основные теоремы, методы и алгоритмы построения классических систем криптографической защиты информации	навыками шифрования и расшифрования в рамках классических систем шифрования
2	Способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	ПК-2	наиболее часто используемые в криптографии программные продукты, инструментальные средства	использовать наиболее часто применяемые в криптографии программные продукты, инструментальные средства	навыками использования наиболее часто применяемых в криптографии программных продуктов и инструментальных средств
3	Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программно-аппаратных и технических средств защиты информации	ПК-6	криптографические методы ЗИ	проводить контрольные проверки работоспособности и эффективности применяемых криптографических средств ЗИ	навыками проведения контрольных проверок работоспособности и эффективности применяемых криптографических средств ЗИ

Содержание разделов дисциплины

№	Наименование и содержание разделов
1	**Раздел 1. Введение в криптографию** История криптографии. Примеры ручных шифров. Основные этапы становления криптографии как науки.
2	**Раздел 2. Математические основы криптографии** Преобразование чисел из одной системы счисления в другую. Кодирование текстов. Элементы теории чисел: НОД, НОК, Простые числа, разложение целого числа на простые множители. Алгоритм Евклида и его значение в криптографии. Элементы теории чисел: Сравнения: Свойства сравнений. Сравнения с одним неизвестным. Системы сравнений. Аффинные преобразования. Частотный криптоанализ. Элементы теории чисел: Классы вычетов: Алгебраические структуры: Группы. Циклическая группа. Алгебраические структуры: Кольцо. Поле Галуа. Поле классов вычетов. Кольцо многочленов. Факториальное кольцо. Евклидово кольцо. Алгебраические структуры: НОД и НОК над конечным полем. Алгоритмы их вычисления. Неприводимые и примитивные многочлены над конечным полем. Односторонние функции.
3	**Раздел 3. Основные задачи и понятия криптографии.** Конфиденциальность, целостность доступность. Атаки, виды атак. Основные требования к шифрам. Основы теории К.Шеннона. Криптографическая стойкость шифров. Теоретически стойкие шифры. Классификация шифров. Шифры с закрытым и открытым ключом и их использование. Простейшие криптографические протоколы. Оценка сложности криптографических алгоритмов
4	**Раздел 4. Основные классы шифров и их свойства** Принципы построения алгоритмов блочного шифрования. Принципы построения алгоритмов поточного шифрования. Шифры перестановки. Шифры простой замены и их анализ. Многоалфавитные шифры замены. Поточные шифры замены. Шифры гаммирования и их анализ. Блочные шифры замены. Блочные шифры простой замены и особенности их анализа. Современные блочные шифры.
5	**Раздел 5. Симметричные шифрсистемы.** Сеть Фейстеля. Криптоалгоритм DES, его разновидности. Криптоалгоритм ГОСТ-28147-89. Режимы работы. Криптоалгоритм RIJNDAEL
6	**Раздел 6. Псевдослучайные генераторы.** Псевдослучайные последовательности (ПСП). Алгоритмы генерации ПСП. Линейные регистры сдвига. Типовые генераторы псевдослучайных последовательностей. Конгруэнтные генераторы. Генераторы Фибоначчи. Генераторы, основанные на сложнорешаемых задачах теории чисел.
7	**Раздел 7. Асимметричные криптосистемы** Системы шифрования с открытым ключом. Шифрсистема RSA. Шифрсистема Эль-Гамаля. Шифрсистема на основе задачи об “укладке рюкзака”. Алгоритмы, основанные на эллиптических кривых. Практические аспекты использования шифрсистем с открытым ключом.
8	**Раздел 8. Алгоритмы распределения ключей.** Алгоритмы передачи ключей (с использованием и без использования цифровой подписи). Алгоритмы открытого распределения ключей. Алгоритмы предварительного распределения ключей.
9	**Раздел 9. Цифровая подпись.** Алгоритмы цифровых подписей. Цифровые подписи на основе шифрсистем с открытым ключом. Цифровая подпись Эль-Гамаля. Стандарты цифровой подписи. Алгоритмы идентификации. Протоколы типа запрос-ответ. Протоколы, использующие цифровую подпись. Протоколы с нулевым разглашением
10	**Раздел 10. Хеш-функции и их криптографические приложения** Хеш-функции и аутентификация сообщений. Общие сведения о хеш-функциях. Ключевые и бесключевые хеш-функции. Понятие о стойкости хеш-функции. Целостность данных и аутентификация источника данных. Конструкции систем аутентификации на основе хеш-функций. Коды аутентичности сообщений: HMAC, UMAC
11	**Раздел 11. Методы криптоанализа. Атаки на шифратор.** Классификация методов криптоанализа. Методы нахождения ключей криптографических алгоритмов. Атаки на шифратор, использующие утечку данных по побочным каналам.

Подробное содержание дисциплины, структура учебных занятий, трудоемкость изучения дисциплины, входные и исходящие компетенции, уровень освоения, определяемый этапом формирования компетенций, учебно-методическое, информационное, материально-техническое обеспечение учебного процесса изложены в рабочей программе дисциплины.