

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования

**«УФИМСКИЙ ГОСУДАРСТВЕННЫЙ АВИАЦИОННЫЙ
ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Кафедра *Вычислительной математики и кибернетики*

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ

УЧЕБНОЙ ДИСЦИПЛИНЫ

« Методы и средства защиты информации »

Уровень подготовки
высшее образование - бакалавриат

Направление подготовки 02.03.03 Математическое обеспечение и администрирование
информационных систем

Квалификация (степень) выпускника
бакалавр

Форма обучения
очная

Уфа 2015

Исполнители:

Доцент, к.т.н.

должность



подпись

Л.Ш.Иванова
расшифровка подписи

Заведующий кафедрой ВМиК



личная подпись

Н.И.Юсупова
расшифровка подписи

Место дисциплины в структуре образовательной программы

Дисциплина «Методы и средства защиты информации» является дисциплиной базовой части ОПОП по направлению подготовки 02.03.03 Математическое обеспечение и администрирование информационных систем.

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки (специальности) 02.03.03 Математическое обеспечение и администрирование информационных систем, утвержденного приказом Министерства образования и науки Российской Федерации от "12" 03. 2015 г. №222.

Задачи курса

- Сформировать представление о назначении, методах и способах защиты информации.
- Изучить криптографические методы защиты информации и стандартные схемы и протоколы защиты
- Изучить принципы защиты средств вычислительной техники от несанкционированного доступа к информации.
- Ознакомиться со структурой, принципами построения и функционирования профилей защиты информационных систем.
- Ознакомиться с общими критериями, предназначенными для использования в качестве основы при оценке характеристик безопасности продуктов и систем информационных технологий

Входные компетенции:

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), практики, научных исследований для которых данная компетенция является входной
1	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-1	<i>Базовый уровень</i>	Метрология и качество ПО / Управление качеством при разработке ПО

Исходящие компетенции

№	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), практики, научных исследований для которых данная компетенция является входной
1	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-1	<i>повышенный</i>	нет

Перечень результатов обучения

Процесс изучения дисциплины направлен на формирование элементов следующих компетенций на базовом уровне.

Планируемые результаты обучения по дисциплине:

№	Формируемые компетенции	Код	Знать	Уметь	Владеть
1	Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-1	Основы криптографии и принципы шифрования	Выявлять источники, риски и формы атак на информацию, разрабатывать политику компании в соответствии со стандартами безопасности, использовать криптографические модели, алгоритмы шифрования информации и аутентификации пользователей, составлять многоуровневую защиту корпоративных сетей.	Средствами и методами защиты информации и применения их на практике в процессе обеспечения защиты информации от вредоносных программ и несанкционированного доступа

Содержание разделов дисциплины

№	Наименование и содержание раздела
---	-----------------------------------

1	Основные понятия защиты информации и информационной безопасности. Анализ угроз. Проблемы безопасности IP-сетей. Пути решения проблем защиты информации в сетях. Политика безопасности
2	Стандарты информационной безопасности. Международные стандарты безопасности. Стандарты информационной безопасности в Интернете. Отечественные стандарты безопасности информационных технологий.
3	Криптографическая защита информации. Симметричные криптосистемы. Блочные шифры. Конструкция Фейстеля. Режимы шифрования блочных шифров. Стандарты блочного шифрования. Стандарт России - ГОСТ 28147-89. Поточные шифры. Шифр RC4.
4	Криптографическая защита информации. Асимметричные криптосистемы. Введение в теорию чисел. Метод распределения ключей Диффи-Хеллмана. Криптосистема RSA. Криптосистема ЭльГамала. Стандарты России ГОСТ 34.10, ГОСТ 34.11
5	Технологии аутентификации. Простая аутентификация. Строгая аутентификация. Биометрическая аутентификация
6	Технологии защиты межсетевого обмена данными. Обеспечение безопасности ОС. Технологии межсетевых экранов.

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.