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

Защита информации

Уровень подготовки: высшее образование – академ. бакалавриат

Направление подготовки
09.03.04 Программная инженерия

Профиль подготовки

Разработка программно-информационных систем

Квалификация (степень) выпускника
Бакалавр
Форма обучения: очная

Уфа 2015

Исполнители:
_____доц. каф. ВМиК_____Иванова Л.Ш.
должность *подпись* *расшифровка подписи*

Заведующий кафедрой ВМиК, проф._____Н.И. Юсупова

Место дисциплины в структуре образовательной программы

Дисциплина «Защита информации» является дисциплиной по выбору вариативной части Б1.В.ОД по направлению подготовки 09.03.04 Программная инженерия и профилю «Разработка программно-информационных систем».

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавра утвержденного постановлением Правительства Российской Федерации от 12.03.2015г. №229.

Целью освоения дисциплины является формирование систематизированных знаний об основах информационной безопасности и защиты информации, о политиках и стандартах безопасности, о технологиях защиты данных; понимания, что без знания и квалифицированного применения современных технологий защиты невозможно достигнуть требуемого уровня информационной безопасности компьютерных систем и сетей.

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
	готовностью применять основные методы и инструменты разработки программного обеспечения	ПК-1	*Базовый уровень*	Проектирование и конструирование программного обеспечения
	способностью осуществлять поиск, хранение, обработку и анализ информации из различных источников и	ПК-4	*Базовый уровень*	Архитектура вычислительных систем и компьютерные сети

	баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий			

Исходящие компетенции

	Компетенция	Код	Уровень освоения, определяемый этапом формирования компетенции	Название дисциплины (модуля), практики, научных исследований для которых данная компетенция является входной
	Владение стандартами и моделями жизненного цикла	ПК-5	*базовый*	Производственная практика, Выпускная квалификационная работа

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
	Владение стандартами и моделями жизненного цикла	ПК-5	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 и структура дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц (144 часов).
Трудоемкость дисциплины по видам работ

Вид работы	Трудоемкость, час.
Лекции (Л)	18
Практические занятия (ПЗ)	
Лабораторные работы (ЛР)	24
КСР	4
Курсовая проект работа (КР)	
Расчетно - графическая работа (РГР)	
Самостоятельная работа (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиумам, рубежному контролю и т.д.)	62
Подготовка и сдача экзамена	
Подготовка и сдача зачета	9
Вид итогового контроля (зачет, экзамен)	зачет

Содержание разделов и формы текущего контроля:

	Наименование и содержание раздела	Количество часов						Литература, рекомендуемая студентам*	Виды интерактивных образовательных технологий**
			Аудиторная работа			РС	Всего		
			З	Р	СР				
	Основные понятия защиты информации и информационной безопасности. Анализ угроз. Проблемы безопасности IP-сетей. Пути решения проблем защиты информации в сетях. Политика безопасности						6	Р 6.1 № 1, гл.1,2,3	*лекция-визуализация, ,*
	Стандарты информационной безопасности. Международные стандарты безопасности. Стандарты информационной безопасности в Интернете. Отечественные стандарты безопасности информационных технологий.						6	Р 6.1 № 1, гл.4 Р 6.2 № 1-5	*лекция-визуализация,*
	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.			2		6	3 4	Р 6.1 № 1, гл.5,6 Р 6.2 № 1	*лекция-визуализация*

	Криптографическая защита информации. Асимметричные криптосистемы. Введение в теорию чисел. Метод распределения ключей Диффи-Хеллмана. Криптосистема RSA. Криптосистема ЭльГамаля. Стандарты России ГОСТ 34.10, ГОСТ 34.11			2		6	3 6	Р 6.1 № 1, гл.5,6 Р 6.2 № 2,3	*лекция-визуализация*
	Технологии аутентификации. Простая аутентификация. Строгая аутентификация. Биометрическая аутентификация					0	1 2	Р 6.1 № 1, гл.7	*лекция-визуализация*
	Технологии защиты межсетевого обмена данными. Обеспечение безопасности ОС. Технологии межсетевых экранов.					2	1 4	Р 6.1 № 1, гл.8,9	*лекция-визуализация*

Занятия, проводимые в интерактивной форме, составляют 100% от общего количества аудиторных часов по дисциплине «Защита информации».

Лабораторные занятия

№ занятия	№ раздела	Тема	Кол-во часов
	3	Симметричные алгоритмы. ГОСТ 28147-89.Режим простой замены	4
	3	Симметричные алгоритмы ГОСТ 28147-89. Гаммирование, гаммирование с обратной связью, имитовставка	4
	3	Потоковые шифры.. Алгоритм RC4	4
	4	Криптосистема RSA	4
	4	Криптосистема ЭльГамаля	4
	4	Цифровая подпись ГОСТ 34.10, ГОСТ 34.11	4

Учебно-методическое и информационное обеспечение дисциплины (модуля)

Основная литература

1. Шаньгин В.Н. Информационная безопасность компьютерных систем и сетей. Москва: Форум, 20111.

2. Борисова С. Н. Методы и средства криптографической защиты данных в вычислительных системах. Часть 2: / Борисова С.Н. - Москва: ПензГТУ (Пензенский государственный технологический университет), 2013.

Основные нормативные акты

1. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

2. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма.

3.ГОСТ Р 34.11-2011. Информационная технология. Криптографическая защита информации. Функция хэширования.

4.ГОСТ Р 50739-95. Защита от несанкционированного доступа к информации

5.ГОСТ Р 51188-98. Испытания программных средств на наличие компьютерных вирусов

Интернет-ресурсы (электронные учебно-методические издания, лицензионное программное обеспечение)

На сайте библиотеки УГАТУ http://library.ugatu.ac.ru/ в разделе «Информационные ресурсы», подраздел «Доступ к БД» размещены ссылки на интернет-ресурсы.

Материально-техническое обеспечение дисциплины

Для проведения *лекций-визуализаций* предусматривается использование специализированного мультимедийного оборудования и интерактивных досок smart board. При реализации педагогической практики с использованием дистанционных образовательных технологий используется действующая в Университете электронно-образовательная среда.

Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.