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

«*ЗАЩИТА ИНФОРМАЦИИ*»

Уровень подготовки
высшее образование – бакалавриат
(высшее образование - бакалавриат; высшее образование – специалитет, магистратура)

Направление подготовки (специальность)
09.03.01 Информатика и вычислительная техника
(код и наименование направления подготовки, специальности)

Направленность подготовки (профиль, специализация)
ЭВМ, системы и сети
(наименование профиля подготовки, специализации)

Квалификация (степень) выпускника
бакалавр

Форма обучения
очная

Уфа 2016

Исполнители:
доцент _____ В.Е.Кладов
должность подпись расшифровка подписи

Заведующий кафедрой
ВТ и ЗИ _____ В.И. Васильев
наименование кафедры *личная подпись* *расшифровка подписи*

Место дисциплины в структуре образовательной программы

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 09.03.01 «*Информатика и вычислительная техника*», утвержденного приказом Министерства образования и науки Российской Федерации от «12» января 2016 г. № 5.

Согласно ФГОС ВО дисциплина «Защита информации» является обязательной дисциплиной вариативной части основной профессиональной образовательной программы (ОПОП) по направлению подготовки бакалавра *09.03.01 Информатика и вычислительная техника*.

Целью освоения дисциплины является формирование у будущих бакалавров в области системного анализа и управления теоретических знаний и практических навыков в области информационной безопасности.

Задачи:

− знание правовых основ и действующих стандартов в области защиты компьютерной информации;

− изучение теоретических основ защиты информации, методов защиты информации, включая криптографические;

− владение практическими навыками в области управления доступом в компьютерных системах.

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-5	Базовый уровень, пятый этап формирования компетенции по аспектам дисциплины	Теория вероятностей и математическая статистика
2	Способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности	ПК-3	Базовый уровень, четвертый этап формирования компетенции по аспектам дисциплины	-
3	использует основные законы естественнонаучных дисциплин в профессиональной деятельности, применяет методы математического анализа и моделирования, теоретического и	ПКП-5	Базовый уровень, шестой этап формирования компетенции по аспектам дисциплины	Теория вероятностей и математическая статистика Моделирование

	экспериментального исследования			

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-5	Базовый уровень, шестой этап формирования компетенции по аспектам дисциплины	Программно-аппаратные средства защиты информации в ЭВМ и системах Проектирование защищенных компьютерных систем
2	Способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности (ПК-3)	ПК-3	Базовый уровень, пятый этап формирования компетенции по аспектам дисциплины	Научно-исследовательская работа
3	использует основные законы естественнонаучных дисциплин в профессиональной деятельности, применяет методы математического анализа и моделирования, теоретического и экспериментального исследования	ПКП-5	Базовый уровень, седьмой этап формирования компетенции по аспектам дисциплины	

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 решать стандартные задачи профессиональной деятельности на основе	ОПК-5	-сервисы информационной безопасности;	-применять знания о способах защиты информации от несанкционированного доступа	- практическими навыками в области управления доступом в

	информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		-систему безопасности операционной системы *Windows*		компьютерных системах; -
	Способность обосновывать принимаемые проектные решения, осуществлять постановку и выполнять эксперименты по проверке их корректности и эффективности	ПК-3	правовые основы и действующие стандарты в области защиты компьютерной информации; математические методы, используемые для анализа стойкости парольных систем	использовать методы организации систем защиты информации; определять параметры контролируемой зоны.	выбора технических и организационных мер по противодействию угрозе -навыками работы с пакетами антивирусных программ
	использует основные законы естественнонаучных дисциплин в профессиональной деятельности, применяет методы математического анализа и моделирования, теоретического и экспериментального исследования	ПКП-5	- терминологию в области защиты информации; - уровни защиты информации; - основные понятия программно-технического уровня информационной безопасности; - основные понятия административного и процедурного уровней информационной безопасности; - криптографические методы защиты информации, распространенные криптографические алгоритмы и особенности их использования;	- применять знания о способах защиты информации от несанкционированного доступа;	- практическими навыками в области управления доступом в компьютерных системах

Содержание и структура дисциплины

Общая трудоемкость дисциплины составляет 6 зачетных единиц (216 часов).

Трудоемкость дисциплины по видам работ

Вид работы	Трудоемкость, час.
	7 семестр 108 часов /3 ЗЕ
Лекции (Л)	18
Практические занятия (ПЗ)	8
Лабораторные работы (ЛР)	20
КСР	3
Самостоятельная работа (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным работам, рубежному контролю и	50

т.д.)	
Подготовка и сдача зачета (контроль)	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				СРС	Всего		
		Л	ПЗ	ЛР	КСР				
1	**Актуальность проблемы защиты информации** Информация и её свойства. Категории информации. Субъекты информационных отношений. Предмет и объект защиты информации. Угрозы безопасности информации в информационно-вычислительных системах (общие понятия). Классификация угроз. Концептуальная модель защиты информации. Структуризация средств обеспечения информационной безопасности (ИБ)	4				12	18	Р 6.1№1, гл. 1	*лекция-визуализация*
2	**Законодательный уровень ЗИ.** Административно-правовая структура ИБ. Интеграция в мировое правовое пространство. **Стандарты:**"Оранжевая книга" - стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем"; Гармонизированные критерии Европейских стран; Международный стандарт ISO/IEC 15408	4	2	4		12	22	Р 6.1№1, гл. 7 Р 6.1 №2, гл. 4	*лекция-визуализация*
3	**Административные меры (**приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами)**.** Политика безопасности и программа безопасности. Синхронизация программы безопасности с жизненным циклом информационных систем. Управление рисками на административном уровне ИБ **Процедурный уровень информационной безопасности:** организация режима работы и охраны предприятия; организацию работы с сотрудниками; организацию работы с	4	2	8		12	26	Р 6.1№1, гл. 7	*лекция-визуализация, анализ конкретных ситуаций* (*кейс* 1)

	документами; организацию использования технических средств; организацию работы по анализу внутренних и внешних угроз								
4	**Программно-технический уровень информационной безопасности** *Основные и вспомогательные сервисы* *Механизмы защиты операционных систем* Каналы утечки информации, обрабатываемой средствами вычислительной техники Стандарты и методы испытаний по ЭМС. *Обеспечение информационной безопасности сетей.* Функционирование сети. Модель OSI. Угрозы и уязвимости проводных корпоративных сетей (КИС). Угрозы и уязвимости беспроводных сетей. Сетевое оборудование. МЭ - пакетный фильтр, функционирующий на сетевом уровне модели OSI.	6	4	8	3	14	33	Р 6.1 №1, гл. 3,4,5 Р 6.1 №2, гл. 2,5,6,8-16 Р 6.2 №1, гл. 1,3,4	*лекция-визуализация*

Занятия, проводимые в интерактивной форме, составляют 47% от общего количества аудиторных часов по дисциплине.

Практические работы

№ занятия	№ раздела	Тема	Кол-во часов
1	2	Законодательный уровень - основа построения системы защиты информации. Российское законодательство в области информационной безопасности	2
1	3	Подбор мер по противодействию угрозам	4
2	4	Изучение математических методов анализа стойкости парольных систем	4

Лабораторные работы

№ занятия	№ раздела	Тема	Кол-во часов
1	**2**	Законодательно-правовое обеспечение информационной безопасности	4
2,3	**4**	Система разграничения доступа и защита данных на сервере MS SQL Server (организация трехуровневого контроля при доступе к объектам БД)	8
4,5	**4**	Автоматизация шифрования	8

Учебно-методическое и информационное обеспечение дисциплины (модуля)

Основная литература

1. Введение в информационную безопасность [Электронный ресурс]: учеб. пособие / А. А. Малюк, В. С. Горбатов, В. И. Королев [и др.]; под ред. В. С. Горбатова - Москва: Горячая линия-Телеком, 2012 - 288 с.

2. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс]: [учебное пособие для студентов высших учебных заведений, обучающихся по направлению «Информатика и вычислительная техника»] / В. Ф. Шаньгин - Москва: ДМК ПРЕСС, 2012 - 592 с.

Дополнительная литература

1. Зайцев А. П. Технические средства и методы защиты информации [Электронный ресурс]: / А. П. Зайцев, Р. В. Мещеряков, А. А. Шелупанов - Москва: Горячая линия-Телеком, 2012 - 442 с.

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

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

Образовательные технологии

При реализации ОПОП дистанционные образовательные технологии, электронное обучение, а также сетевое обучение не реализуются.

Материально-техническое обеспечение дисциплины

Перечень лекционных аудиторий с современными средствами демонстрации – 5-301, 5-314.

Перечень лабораторий современного, высокотехнологичного оборудования, обеспечивающего реализацию ОПОП ВО с учетом направленности подготовки:

- 5-313 – дисплейный класс;

Вычислительное и телекоммуникационное оборудование и программные средства, необходимых для реализации ОПОП ВО и обеспечения физического доступа к информационным сетям, используемым в образовательном процессе и научно-исследовательской деятельности:

- компьютерная техника:
  - Intel Core i7-4790/ASUS Z97-K DDR3 ATX SATA3/Kingston DDR-III 2x4Gb 1600MHz/Segate 1Tb SATA-III/ Kingston SSD Disk 240Gb; серверы: CPU Intel Xenon E3-1240 V3 3.4GHz/4core/1+8Mb/80W/5GT ASUS P9D-C /4L LGA1150 / PCI-E SVGA 4xGbLAN SATA ATX 4DDR-III HDD 3 Tb SATA 6Gb/s Seagate Constellation CS 3,5" 7200rpm 64 Mb Crucia <CT102472BD160B> DDR-III DIMM 2x8Gb <ST3000NC002> CL11;
- программное обеспечение:
  - Программный комплекс – операционная система Microsoft Windows (№ договора ЭФ-193/0503-14, 1800 компьютеров, на которые распространяется право пользования)
  - Программный комплекс – Microsoft Office (№ договора ЭФ-193/0503-14, 1800 компьютеров, на которые распространяется право пользования)
  - Программный комплекс – Microsoft Project Professional (№ договора ЭФ-193/0503-14, 50 компьютеров, на которые распространяется право пользования)
  - Программный комплекс – операционная система Microsoft Visio Pro (№ договора ЭФ-193/0503-14, 50 компьютеров, на которые распространяется право пользования)
  - Kaspersky Endpoint Security для бизнеса (лицензии 13C8-140128-132040, 500 users).
  - Dr.Web® Desktop Security Suite (КЗ) +ЦУ (AH99-VCUN-TPPJ-6k3L, 415 рабочих станций).
  - ESET Smart Security Business (EAV-8424791, 500 пользователей).
  - Контур информационной безопасности SearchInform (UEI-2349-87, 25 пользователей).
  - Secret Net (IEK-109869, 25пользователей).
  - InfoWatch Traffic Monitor Enterprise (IWES-S3-DE, 25пользователей).
  - Seagate Central Discovery для ОС Windows (WOS-65-GT5, 25пользователей).

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.