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

«СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И АУДИТ»

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 «Стандарты информационной безопасности и аудит» 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.

Целью освоения дисциплины является приобретение студентами знаний по отечественной и зарубежной системам стандартов в области информационной безопасности. Овладение навыками анализа и применения положений стандартов в области информационной безопасности, а также методами и методиками проведения аудита информационных систем.

Цели освоения дисциплины – приобретение студентами знаний по отечественной и зарубежной системам стандартов в области информационной безопасности. Овладение навыками анализа и применения положений стандартов в области информационной безопасности, а также методами и методиками проведения аудита информационных систем.

Задачи:

- сформировать знания об отечественной и зарубежной системах стандартов в области информационной безопасности;
- изучить основные стандарты в области информационной безопасности;
- сформировать представление у студентов о существующих методах и методиках проведения аудита информационных систем;
- изучить особенности проведения аудита различных информационных систем.

Предшествующими курсами, на которых непосредственно базируется дисциплина «Стандарты информационной безопасности и аудит», являются: «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности».

Вместе с тем курс «Стандарты информационной безопасности и аудит» является основополагающим для изучения дисциплины «Комплексная система защиты информации на предприятии», а также при разработке курсовых и выпускных квалификационных работ.

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 принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности	ПК-5	- основные международные и национальные стандарты, регламентирующие деятельность в области информационной безопасности;	- использовать стандарты информационной безопасности для аттестации объектов на предмет соответствия требованиям защиты информации;	- методами проведения аттестации на предмет соответствия требованиям защиты информации; - анализа активов организации, угроз информаци-

	информации		- руководящие документы и стандарты по аттестации	- анализировать текущее состояние информационной безопасности в организации с целью разработки требований к разрабатываемым процессам управления информационной безопасностью	онной безопасности и уязвимостей
2.	Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	ПК-10	- основные международные и национальные стандарты, регламентирующие деятельность в области информационной безопасности	- анализировать текущее состояние информационной безопасности в организации с целью разработки требований к разрабатываемым процессам управления информационной безопасностью	- анализа активов организации, угроз информационной безопасности и уязвимостей

Содержание разделов дисциплины

№	Наименование и содержание разделов
1	**Стандарты в области информационной безопасности** Стандарты в области управления информационной безопасностью. Структура международных стандартов по ИБ. Область применения. Процессная модель управления ИБ. Взаимосвязь стандартов. Цели управления, меры и средства управления ИБ. Подходы к оценке системы управления ИБ. Оценка зрелости системы управления ИБ. ISO 27001 (BS 7799 – 2:2005). Управление рисками информационной безопасности. Анализ рисков: различные определения и постановки задач. Разработка корпоративной методики анализа рисков: постановка задачи; этапы анализа риска; управление рисками. Технологии анализа рисков: идентификация рисков; подходы к оцениванию рисков; объективные и субъективные вероятности; получение оценок субъективной вероятности. Методология измерения рисков: оценка рисков по двум факторам; оценка рисков по трем факторам; выбор допустимого уровня риска. Выбор контрмер и оценка их эффективности. Другие стандарты: ГОСТ Р ИСО/МЭК 15408 (“Общие критерии”). ГОСТ Р ИСО/МЭК 17799. Руководящие документы ФСТЭК России и аудит в целях сертификации средств защиты и аттестации объектов информатизации.
2	**Аудит информационной безопасности компании: общие понятия и определения** Понятия аудита ИБ. Виды аудита. Внешний и внутренний аудит. Необходимость и актуальность аудита безопасности. Постановка проблемы аудита безопасности. Оценка состояния ИБ. Цели и задачи аудита ИБ. Особенности автоматизированных информационных систем как объектов аудита ИБ.

3	**Методология аудита информационной безопасности. Организация процесса аудита.** Основные этапы и методы работ по проведению аудита безопасности. Этапы проведения аудита. Стадии аудита: планирование; моделирование; тестирование; анализ; разработка предложений; документирование. Методы аудита: экспертно-аналитические; экспертно-инструментальные; моделирование действий злоумышленника (“взлом” защиты информации). Сбор исходной информации для проведения аудита. Цель сбора исходных данных. Методы сбора исходных данных. Общие исходные данные. Исходные данные об обрабатываемой информации. Исходные данные о системе обеспечения безопасности информации. Исходные данные о персонале. Сбор дополнительных исходных данных. Анализ значимости информационных ресурсов. Моделирование действий злоумышленника (“взлом” защиты информации). Рекомендации по анализу и документированию результатов. Цель и методы обследования на этапе анализа. Анализ организационно-распорядительных документов, выполнения организационно-технических требований, деятельности персонала (сотрудников). Отчетные материалы.
4	**Инструментальные средства аудита ИБ** Методы и инструментальные средства проведения активного аудита ИБ. Обнаружение и устранение уязвимостей. Возможности сканеров безопасности. Программные средства анализа и управления рисками. Инструментарий базового уровня: справочные и методические материалы; ПО идентификации и оценки защищаемых ресурсов, угроз, уязвимостей и мер защиты в сфере компьютерной и “физической” безопасности предприятия. RiskWatch; средства анализа и управления рисками CRAMM; комплексная система анализа и управления рисками информационной системы компании ГРИФ; комплексная экспертная система управления информационной безопасностью “РискМенеджер”.

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.