

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

«ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ»

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

Место дисциплины в структуре образовательной программы

Дисциплина «Проектирование защищенных компьютерных систем» 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 формирование систематизированных знаний о процессах разработки защищенных компьютерных систем и систем защиты информации, применяемых при этом подходах, методиках и механизмах защиты информации, а также формирование у обучающихся умений и навыков, необходимых при непосредственном участии в указанных процессах.

Задачи:

- Сформировать знания о моделях и этапах жизненного цикла защищенных компьютерных систем и систем защиты информации, применяемых подходах и методах по обеспечению безопасности на каждом из этапов.

- Сформировать представления об уязвимостях, присущих компьютерным системам, связанных с ними угрозами, а также навыки формирования моделей угроз безопасности и моделей потенциальных нарушителей.

- Сформировать и развить компетенции, знания и практические навыки обеспечения технологической и эксплуатационной безопасности компьютерных систем.

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 определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	ОПК-7	- методики анализа и моделирования угроз безопасности информации; - методы анализа рисков информационной безопасности; - технологию определения состава защищаемых информационных ресурсов	- проводить обследование компьютерных систем и документировать его результаты; - анализировать уязвимости компьютерных систем и находить пути их нейтрализации	- методами и инструментами обследования компьютерных систем и анализа их защищенности
2	Способность проводить анализ исходных данных для	ПК-7	- методы анализа рисков информационной безопас-	- систематизировать и описывать требования к механизмам и	- инструментами анализа рисков информационной без-

	проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений		ности; - методики формирования требований к механизмам и средствам защиты информации	средства защиты информации; - готовить техническое задание и технико-экономическое обоснование на системы защиты	опасности
3	Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ПК-8	- технологию анализа и моделирования угроз безопасности информации; - методы и средства обеспечения безопасности в компьютерных системах; - отечественные и зарубежные нормативные документы и стандарты, определяющие основные требования к разработке и проектированию защищенных компьютерных систем	- разрабатывать структуру и определять состав подсистем информационной безопасности компьютерных систем и систем защиты информации	- современными методами и средствами системного моделирования

Содержание разделов дисциплины

№	Наименование и содержание разделов
1	Компьютерная система как объект защиты: Понятие, структура и состав компьютерной системы. Классификация информационных систем с точки зрения безопасности. Принципы обеспечения информационной безопасности. Российские и зарубежные подходы к определению защищенной компьютерной системы. Жизненный цикл компьютерной системы. Модели жизненного цикла компьютерной системы.
2	Проектирование защищенных компьютерных систем: Этапы разработки защищенной компьютерной системы. Формирование требований к компьютерной системе. Моделирование угроз технологической безопасности компьютерной системы. Подходы к моделированию компьютерных систем. Объектно-ориентированное моделирование, язык UML. Управление проектированием защищенных компьютерных систем. Методы обеспечения защищенности компьютерной системы на этапе кодирования и тестирования.
3	Проектирование систем защиты информации: Структура и назначение системы защиты информации. Этапы построения системы защиты информации. Порядок разработки системы защиты персональных данных. Порядок разработки системы защиты информации в государственной информационной системе. Порядок разработки системы защиты информации в АСУ ТП. Оценка соответствия системы защиты. Методики анализа рисков информационной безопасности. Аттестации информационной системы по безопасности.

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.