

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

***«ТЕОРИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОЛОГИЯ
ЗАЩИТЫ ИНФОРМАЦИИ»***

Уровень подготовки: высшее образование – специалитет

Специальность

10.05.05 «Безопасность информационных технологий
в правоохранительной сфере»
(код и наименование специальности)

Специализация

Технологии защиты информации в правоохранительной сфере
(наименование специализации)

Квалификация (степень) выпускника

Специалист

Форма обучения - очная

Год начала подготовки – 2013

Место дисциплины в структуре образовательной программы

Дисциплина «Теория информационной безопасности и методология защиты информации» является дисциплиной базовой части основной образовательной программы (ОПОП).

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего профессионального образования по специальности 090915 Безопасность информационных технологий в правоохранительной сфере, утвержденного приказом Министерства образования и науки Российской Федерации от "01" февраля 2011 г. № 132, 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 специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, утвержденного приказом Министерства образования и науки Российской Федерации 19 декабря 2016 г. № 1612. Является неотъемлемой частью основной профессиональной образовательной программы.

Целью освоения дисциплины является формирование компетенций в области информационной безопасности, включая знания, умения, навыки и социально-личностные качества, обеспечивающие развитие творческих подходов при решении задач, связанных с обеспечением безопасности информационных систем.

Задачи:

1. Сформировать комплекс базовых знаний в области теории информационной безопасности и методологии защиты информации.
2. Сформировать и развить практические навыки и умения, способствующие всестороннему и эффективному применению современных методов анализа и проектирования защищенных информационных 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 выявлять естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности и использовать общенаучные методы, законы физики, математический аппарат, методы моделирования и прогнозирования развития процессов и явлений при решении профессиональных задач	ОПК-1	- базовый понятийный аппарат в области информационной безопасности; - критерии, условия и принципы отнесения информации к защищаемой	- определять виды и состав угроз информационной безопасности	- навыками формальной постановки и решения задачи обеспечения информационной безопасности
2.	Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	ПК-1	- направления обеспечения безопасности информации; - современные подходы к построению систем защиты информации	- определять политику безопасности информационных систем	Навыками использования современных программно-аппаратных средств защиты

3.	Способность принимать участие в создании системы защиты информации на объекте информатизации	ПК-31	- особенности обеспечения безопасности информационной систем - методики оценки защищенности информационных систем	- пользоваться современной научно-технической информацией по исследуемым проблемам и задачам	- навыками использования методов анализа и оценки угроз безопасности защищаемой информации
----	--	-------	--	--	--

Содержание разделов дисциплины

№	Наименование и содержание разделов
1	Теоретические и концептуальные основы защиты информации. Понятие и назначение теории защиты информации. Основные положения теории защиты информации. Связь информационной безопасности с информатизацией общества. Современная стратегия защиты информации. Концептуальная модель информационной безопасности.
2	Направления, методы и средства защиты информации. Виды защиты информации, сферы их действия. Классификация методов защиты информации. Области применения организационных, правовых и инженерно-технических методов защиты информации. Модель злоумышленника.
3	Информационное воздействие. Воздействующая роль информации. Информационные технологии воздействия. Информационная экология. Средства информационно-технического и информационно-психологического воздействия.
4	Оценка информационной безопасности предприятия. Политика безопасности предприятия. Понятие информационного риска. Методики анализа информационных рисков.

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.