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

«ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

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 «Техническая защита информации» относится к обязательным дисциплинам 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.

Цели освоения дисциплины – формирование понятийного аппарата, методологической базы, учитывающей специфику защиты информации в организации, систематизированных и структурированных знаний о принципах добывания информации по техническим каналам и характеристиках технических каналов ее утечки, способах и средствах защиты информации.

Задачи:

– сформировать знания о свойствах информации как предмета защиты, видах защищаемой информации, об источниках и носителях информации;

– изучить виды угроз безопасности информации, способы ее добывания путем несанкционированного доступа;

– изучить особенности утечки информации, характеристики технических каналов утечки информации: оптических, радиоэлектронных, акустических, материально-вещественных;

– сформировать представление у студентов о заходовых и беззаходовых способах перехвата сигналов, средствах акустического контроля помещений; способах и средствах наблюдения в оптическом- и радиодиапазонах;

– изучить общие положения по технической защите информации в организациях, организационные и технические меры, методическое обеспечение технической защиты информации, включая моделирование объектов защиты и угроз;

– изучить измерительные и поисковые технические средства и методы их применения с целью инструментального выявления каналов утечки информации, определения зон безопасности объектов;

– изучить методы защиты помещений объектов информатизации от утечки информации по техническим каналам, а также современную номенклатуру применяемых технических средств защиты и материалов.

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 применять положения электротехники, электроники и схемотехники для решения профессиональных задач	ОПК-3	- свойства информации как предмета защиты, виды защищаемой информации, источники и носители информации, характеристики технических каналов утечки информации	- использовать измерительные и поисковые технические средства и методы с целью инструментального выявления каналов утечки информации	

2	Способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	ПК-1	- современную номенклатуру применяемых технических средств защиты и материалов		- методами защиты помещений, объектов информатизации от утечки информации по техническим каналам
3	Способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации	ПК-6	- положения по технической защите информации в РФ и организациях	- использовать измерительные и поисковые технические средства и методы с целью инструментального выявления каналов утечки информации	- методами определения зон безопасности объектов информатизации
4	Способность принимать участие в проведении экспериментальных исследований системы защиты информации	ПК-12	- заходовые и беззаходовые способы перехвата сигналов, средства акустического контроля помещений; способы и средства наблюдения в оптическом- и радиодиапазонах	- использовать измерительные и поисковые технические средства и методы с целью инструментального выявления каналов утечки информации	- методами определения зон безопасности объектов инфоратизации
5	Способность принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	ПК-13	- виды угроз безопасности информации, способы ее добывания путем несанкционированного доступа	- составлять модели объектов защиты и модели угроз информации	

Содержание разделов дисциплины

№	Наименование и содержание разделов
1	**Основные направления ИТЗИ:** 1) Цели, задачи, принципы ИТЗИ. Системный подход к ИТЗИ. Мероприятия и методы по технической защите информации. 2) Угрозы безопасности информации, источники угроз. Факторы, воздействующие на информацию
2	**Общие представления о защищаемой информации:** 1) Понятие об информации как об объекте защиты. Основные свойства информации как объекта защиты. Виды защищаемой информации. 2) Демаскирующие признаки объектов защиты. Классификация демаскирующих признаков. Видовые демаскирующие признаки. Демаскирующие признаки веществ, сигналов. Параметры измеряемых сигналов. Источники и носители информации. 3) Источники опасных функциональных и случайных сигналов. Составление структурных моделей «Источники сигналов» и «Факторы, воздействующие на информацию»

№	Наименование и содержание разделов
3	**Технические каналы утечки информации:** 1) Структура, классификация и краткая характеристика технических каналов утечки информации. 2) ТКУИ за счет ПЭМИН ТСОПИ (электромагнитные каналы утечки, наводки в цепях питания и заземления ТСОПИ, акустоэлектрические преобразования и паразитные высокочастотные генерации в схемах ТСОПИ). Параметрические каналы утечки информации. Информативные излучения и токи утечки линий электросвязи. 3) Визуально-оптические и оптоэлектронные каналы утечки информации. Информативные излучения ВОЛС. 4) Акустические и виброакустические каналы утечки информации (структура акустического (виброакустического) канала утечки информации, источники акустического сигнала, особенности распространения акустических сигналов в различных средах, качество подслушанной речи, модель ВАКУИ из помещений). 5) Вещественные каналы утечки информации.
4	**Способы и специальные технические средства добывания информации:** 1) Специальные технические средства, общие сведения. Классификация закладочных устройств. 2) Способы и средства, предназначенные для негласного получения и регистрации акустической информации (средства для наблюдения заходовым способом – микрофоны линейные и радио-, диктофоны, средства для наблюдения беззаходовым способом – направленные микрофоны и лазерные микрофоны). 3) Основные методы прослушивания телефонных линий (способы подключения телефонной линии и запись переговоров, перехват разговоров в помещении через схему ТА). 4) Способы и средства, предназначенные для негласного визуального наблюдения (средства для наблюдения заходовым способом – малогабаритные устройства видеонаблюдения и видеозаписи, средства для наблюдения беззаходовым способом – оптические линзовые и оптоэлектронные устройства).
5	**Организация и методическое обеспечение ИТЗИ** 1) Общие положения по технической защите информации в организациях. Нормативно-методическое обеспечение СЗИ предприятия. Основные этапы проектирования системы защиты информации техническими средствами. Организация работ по лицензированию и сертификации в области защиты информации. 2) Моделирование объектов защиты (моделирование угроз безопасности информации, моделирование способов физического проникновения злоумышленника к источникам информации, моделирование технических каналов утечки информации).
6	**Радиоэлектронное противодействие и радиомаскировка:** 1) Противодействие техническим разведкам, общие сведения. Концепция ИТЗИ. 2) Радиомаскировка пассивная (экранирование, фильтрация, заземление. специальные помещения, специальные пассивные методы защиты кабельных линий, соединительных проводов, защищенные ТСОПИ). 3) Радиомаскировка активная (помехи, показатель эффективности радиомаскировки ПЭМИН, радиомаскировка ПЭМИ средств ЭВТ, схемы реализации электромагнитного зашумления, защита внешних линий ТСОПИ, средства шифрования). 4) Средства и методы СИ ТСОПИ на соответствие нормам эффективности защиты
7	**Противодействие акустической речевой разведке:** 1) Показатель противодействия речевой разведке. Способы противодействия. 2) Средства и методы пассивной защиты помещений (звукоизоляция, специальные конструкции помещений и коммуникаций, проектирование защищенных помещений). 3) Средства и методы активной защиты помещений (генераторы акустического шума, противодействие негласному использованию подслушивающих устройств). 4) Средства и методы противодействия разведке объектов информатизации с использованием закладочных устройств (выявление подслушивающих и видео- устройств).

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.