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

«ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА 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

Уфа 2017

Место дисциплины в структуре образовательной программы

Дисциплина «Инженерно-техническая защита информации» является дисциплиной базовой части основной профессиональной 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 понятийного аппарата, методологической базы, учитывающей специфику защиты информации в правоохранительной сфере, 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 источников сигналов и угроз безопасности информации, способы несанкционированного доступа к источникам сигналов, моделирование объектов защиты и угроз;

– изучить особенности утечки информации по различным физическим средам, характеристики технических каналов утечки информации (ТКУИ), принципы и технологии добывания информации с пощью технических средств разведки (ТСР), сформировать представление у студентов о современных средствах и системах технической разведки (ТР);

– изучить общие положения по инженерно-технической защите информации (ИТЗИ) в организациях, организационные и технические меры, методическое обеспечение ИТЗИ,

– изучить способы реализации ИТЗИ объектов информатизации от утечки и добывания информации по техническим каналам утечки информации (ТКУИ), а также современную номенклатуру применяемых технических средств защиты и материалов;

– изучить средства и методы: инструментального контроля показателей эффективности защиты объектов информатизации от утечки информации по ТКУИ, применяемые в ходе специальных исследований (СИ) и специальных проверок (СП), определения зон безопасности объектов по нормам эффективности защиты.

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 формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечи-	ПК-1	– принципы ИТЗИ, основные направления ведения технической разведки	– применять методы анализа объектов защиты, включая методы моделирования объек-	- методами выявления и оценки угроз безопасности защищаемой

	вать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз		(ТР) и способы противодействия ей; – технологию определения состава и категорию защищаемой информации в зависимости от ее важности на объектах защиты; – методы моделирования объекта защиты и ТКУИ.	тов защиты и ТКУИ; - выявлять угрозы безопасности защищаемой информации по демаскирующим признакам, строить модели: физического проникновения злоумышленника и ТКУИ, с учетом решаемых задач и структуры объекта защиты.	информации для конкретного объекта информатизации, выбора адекватных мер технической защиты информации для конкретного объекта защиты
2	Способность применять технические и программно-аппаратные средства обработки и защиты информации	ПК-2	– состав и технические характеристики современных средств защиты информации и материалов.	– применять материалы и средства защиты информации от средств технической разведки и за счет непреднамеренного перехвата.	- способами реализации систем инженерно-технической защиты информации
3	Способность принимать участие в создании системы защиты информации на объекте информатизации	ПК-31	– методы и средства выявления ТКУИ на объекте информатизации; – методы инжнерно-технической защиты информации, номенклатуру средств и материалов применяемых для защиты объектов информатизации от технических средств разведки; – методы инструментального контроля эффективности защиты информации.	– определять основные информативные параметры физических полей; – пользоваться инструментальными средствами для выявления и измерения КУИ по различным физиическим полям, рассчттывать размеры зон безопасности объектов защиты, защитные мероприятия.	– способами инструментального определения норм эффективности защиты информации от утечки по техническим каналам; .

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) Классификация и характеристика технических каналов перехвата информации при ее передаче по каналам радио- и электросвязи в открытом режиме (классификация линий и каналов связи, принципы построения МКСС, характеристики кабельных линий связи и радиоканалов). 6) Вещественные каналы утечки информации.
4	**Технология, способы и средства добывания информации:** 1) Разведывательный цикл. Технология добывания информации. Способы и средства доступа органов добывания (злоумышленников) к источникам информации. 2) Основные подходы к построению систем РЭР для реализации перехвата информативных ПЭМИН (заметность радиоизлучений, зоны разведдоступности, оптимальный приемник разведки, выделение информативного излучения на фоне объектовой помехи, возможность восстановления перехваченных сигналов). 3) Способы и средства наблюдения в оптическом диапазоне (линзовые системы, угол зрения, разрешение и увеличение, параметры объективов, визуально-оптические приборы, средства видео- и телевизионного наблюдения, электронно-оптические преобразователи). 4) Способы и средства подслушивания (сравнительные возможности слуха и электроакустических преобразователей при подслушивании разговоров, микрофоны и вибропреобразователи, чувствительность и отдача микрофонов, классификация и конструкции, обобщенная модель речевой разведки).
5	**Современные разведывательные устройства и системы:** 1) Общие сведения о технических разведках. Классификация ТР по каналам добывания информации и носителям аппаратуры разведки. 2) Радиоэлектронная разведка. Радио и радиотехническая разведка. Радиолокационная разведка. Радиотепловая разведка. Разведка ПЭМИН. 3) Оптическая и оптико-электронная разведки. Визуально-оптическая разведка. Фотографическая и фототелевизионная разведка. Разведка в ИК диапазоне. Тепловидение. Теплопеленгация. Лазерная локация. 4) Акустическая речевая разведка (средства и методы ведения акустической речевой разведки). 5) Гидроакустическая разведка (особенности распространения акустических волн в воде, гидролокация и гидрофония). 6) Компьютерная разведка (методы взлома компьютерных систем, программы шпионы). 7) Деструктивное воздействие на ТСОПИ (основные каналы СДВ, Классификация средств силового деструктивного воздействия на интегрированные системы безопасности).
6	**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).
7	**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,

№	Наименование и содержание разделов
	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) Предотвращение утечки информации хранящейся на магнитных накопителях. Защита от деструктивного воздействия на СВТ. 5) Средства и методы оценки радиотехнической безопасности объекта информатизации (задачи, методы и средства радиомониторинга, специальные исследования и проверки ТСОПИ).
8	**Противодействие акустической речевой разведке:** 1) Показатель противодействия речевой разведке. Способы противодействия. 2) Средства и методы оценки защищенности помещений от утечки речевой информации по акустическим и вибрационным каналам. 3) Средства и методы пассивной защиты помещений (звукоизоляция, специальные конструкции помещений и коммуникаций, проектирование защищенных помещений). 4) Средства и методы активной защиты помещений (генераторы акустического шума, противодействие негласному использованию подслушивающих устройств). 5) Средства и методы оценки защищенности помещений от утечки информации за счет акустоэлектрических преобразований в схемах ТСОПИ. Методы защиты линий ВТС.

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.