Аннотация к рабочей программе дисциплины

«Защита информации от технической разведки»

Рабочая программа учебной дисциплины «Защита информации от технической разведки» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин вариативной части учебного плана Б1В.05.

Общая трудоемкость освоения дисциплины составляет 5 зачетных единицы, 180 академических часа. Учебным планом предусмотрены лекционные занятия (36 часов), лабораторные работы (54 часов), практические занятия (36 часов), самостоятельная работа (54 часов). Дисциплина реализуется на 5 курсе, в А семестре. Форма контроля по дисциплине – экзамен.

Дисциплина «Защита информации от технической разведки» основана на предварительном изучении следующих дисциплин: «Информатика», «Основы информационной безопасности», «Модели безопасности компьютерных систем», «Аппаратные средства вычислительной техники», «Защита программ и данных». Знания и практические навыки, полученные при изучении дисциплины «Защита информации от технической разведки», обеспечивают освоение следующих дисциплин: «Инженерная защита и охрана объектов», «Программно-аппаратные средства обеспечения информационной безопасности», «Теория и проектирование защищенных систем».

Дисциплина имеет практическую направленность, при этом большое значение для освоения дисциплины имеют лабораторные занятия. В ходе реализации дисциплины в рамках лекционных, лабораторных и практических занятий применяются методы активного/ интерактивного обучения, реализующие наглядное представление результатов защиты информации от технической разведки.

Дисциплина «Защита информации от технической разведки»

обеспечивает приобретение знаний и умений в области технической разведки, а также обеспечения защиты информации от средств технической разведки. Изучение этой дисциплины способствует освоению способов и средств защиты выявленных каналов добывания информации.

Цель дисциплины – раскрыть природу ведения технической разведки, сформировать представление о проблемах защиты информации от технической разведки, выработать умения и навыки применению средств защиты информации от технической разведки, сформировать умения по выработке рекомендаций по защите от технической разведки.

Задачи:

- изучить основных угроз безопасности информации и модели нарушителя в КС;
- изучить основные этапы и процедуры добывания информации технической разведки;
- освоить методы спектрального анализа с помощью пакета прикладных программ MATLAB;
- изучить методы работы с комплексом выявления технических каналов утечки информации;
- изучить возможность выявления каналов утечки информации нелинейным локатором NR-900EM;
- оценить защищенность информации, обрабатываемой ТСПИ, от утечки по каналу ПЭМИ.

Для успешного изучения дисциплины «Защита информации от технической разведки» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);

•способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3);

•способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения (ОПК-7);

•способность производить установку, наладку, тестирование и обслуживание современного общего и специального программного обеспечения, включая операционные системы, системы управления базами данных, сетевое программное обеспечение (ПК-17).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ПК-12) способность проводить инструментальный мониторинг защищенности компьютерных систем	Знает	особенности каналов утечки информации в компьютерных системах, методы и технические перекрытия этих каналов
	Умеет	анализировать каналы утечки информации, возможные в конкретной компьютерной системе, организовывать защиту информации в ней
	Владеет	программными и техническими средствами защиты информации в компьютерных системах
(ПК-14) способность организовывать работы по выполнению режима защиты информации, в том	Знает	организационные, программные и технические методы защиты информации
	Умеет	анализировать уровень защищённости информации в различных её проявлениях с привязкой к конкретным

числе ограниченного доступа		реальным условиям
	Владеет	методами и практическими навыками анализа создания систем защиты информации
(ПК-20) способность выполнять работы по восстановлению работоспособности средств защиты информации при возникновении нештатных ситуаций	Знает	методы технической и программной защиты информации
	Умеет	тестировать конкретные компьютерные системы с использованием аппаратных и программных средств на предмет уровня защищённости информации в них и в помещениях где они расположены
	Владеет	программными и аппаратными средствами контроля защиты информации

Для формирования вышеуказанных компетенций в рамках дисциплины «Защита информации от технической разведки» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6), конспект (ПР-7).