АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«ТЕХНИЧЕСКИЕ СРЕДСТВА ОБНАРУЖЕНИЯ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ»

по специальности 10.05.03 «Информационная безопасность автоматизированных систем» специализация «Безопасность открытых информационных систем»

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учебная дисциплина «Технические средства обнаружения каналов утечки информации» обеспечивает приобретение знаний и умений в соответствии с государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Цель курса – ознакомление студентов с основными техническими средствами обнаружения каналов утечки информации.

Задачи:

− изучение способов и средств обнаружения каналов утечки информации;

− изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Технические средства обнаружения каналов утечки информации» относится к числу прикладных дисциплин и занимает важное место в блоке дисциплин по выбору Б1.В.1.ДВ, предназначенных для подготовки студентов по специальности – 10.05.03 "Информационная безопасность автоматизированных систем".

Для успешного изучения дисциплины необходимы знания и умения, приобретенные в результате освоения курсов «Физика», «Техническая защита информации», «Безопасность операционных систем», «Основы информационной безопасности», «Электроника и схемотехника».

Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции:

- способность анализировать социально-значимые проблемы и процессы;
- знание базовых понятий в области физики, вычислительной техники, электроники и схемотехники;
- способность использовать основные законы естественнонаучных дисциплин, применять методы математического анализа и моделирования.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин, как: «Безопасность вычислительных сетей»; «Разработка и эксплуатация автоматизированных систем в защищённом исполнении», «Безопасность открытых информационных систем», а в части выявления технических каналов утечки информации объекта информатизации, на дисциплинах, изучающих методы и средства защиты информации.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СОТНЕСЕНЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Процесс изучения дисциплины направлен на формирование следующих компетенций:

Код и наименование реализуемой	Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с

компетенции	индикаторами достижения компетенций
1	2
ПК-1 - Способен организовать работы по выполнению в информационной системе требований защиты информации ограниченного доступа	**Знать:** Источники и классификацию угроз информационной безопасности Основные средства и способы обеспечения информационной безопасности, принципы построения систем защиты информации Нормативные правовые акты в области защиты информации **Уметь:** Классифицировать и оценивать угрозы информационной безопасности для объекта информатизации Организовывать реализацию мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты Организовывать процесс применения защищенных протоколов, межсетевых экранов, средств обнаружения вторжений для защиты информации в сетях **Владеть:** Навыками организации применения защищенных протоколов, межсетевых экранов и средств обнаружения вторжений для защиты информации в сетях Навыками управления процессом разработки моделей угроз и моделей нарушителя безопасности компьютерных систем
ПК-2 - Способен осуществлять тестирование систем защиты информации автоматизированных систем	**Знает:** Принципы построения и функционирования систем и сетей передачи информации Эталонную модель взаимодействия открытых систем Основные криптографические методы, алгоритмы, протоколы, используемые для защиты информации в автоматизированных системах **Умеет:** Применять действующую нормативную базу в области обеспечения безопасности информации Контролировать безотказное функционирование технических средств защиты информации **Владеет:** Навыками подбора инструментальных средств тестирования систем защиты информации автоматизированных систем
ПК-6 - Способен проводить контроль защищенности информации от НСД	**Знать:** Методы защиты информации от несанкционированного доступа и специальных программных воздействий на нее Методы и методики контроля защищенности информации от несанкционированного доступа и специальных программных воздействий **Уметь:** Проводить оценку защищенности информации от

	несанкционированного доступа и специальных воздействий Проверять работоспособность средств защиты информации от несанкционированного доступа и специальных воздействий, выполнение правил их эксплуатации **Владеть:** Навыками проведения контроля защищенности информации от несанкционированного доступа и специальных воздействий

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 5 зачетных единиц (180 часов).

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В ходе освоения дисциплины при проведении аудиторных занятий используются следующие образовательные технологии: лекционные занятия, интерактивный опрос в ходе лекций, эвристическая беседа, диалог, ознакомительные беседы с представителями потенциальных работодателей.

При организации самостоятельной работы занятий используются образовательные технологии развивающего, проблемного и проектного обучения.

6. КОНТРОЛЬ УСПЕВАЕМОСТИ

Программой дисциплины предусмотрены следующие виды текущего контроля: письменные и устные опросы на лекциях, лабораторных работах, в ходе написания рефератов.

Промежуточная аттестация проводится в форме зачёта и экзамена.