АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
«ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ»

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

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Учебная дисциплина «Техническая защита информации»обеспечивает приобретение знаний и умений в соответствии с федеральным государственным образовательным стандартом, содействует формированию мировоззрения и системного мышления.

Целью дисциплины «Техническая защита информации» является формирование у студентов знаний по основам технической защиты информации, а также навыков и умений в применении знаний для конкретных условий. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач технической защиты информации с учетом требований системного подхода.

Основные задачи дисциплины – дать знания:

- по концепции и организационным основам инженерно-технической защиты информации;
- теоретическим и физическим основам технической защиты информации;
- по техническим средствам добывания и защиты информации;
- по методическому обеспечению технической защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Техническая защита информации» относится к числу дисциплинбазового блока и занимает важное место в рамках образовательной программы подготовки по специальности – "Информационная безопасность автоматизированных систем".

Дисциплина читается в 6-ом семестре студентам 3-го курса очной формы обучения и базируется на знаниях и умениях, приобретённых в результате освоения дисциплин: «Физика», «Электроника и схемотехника», «Безопасность операционных систем», «Основы информационной безопасности», позволяющими понять физическую сущность возникновения технических каналов утечки информации, возможности современных средств технической разведки, методы и способы защиты от утечки по техническим каналам.

Основные положения дисциплины используются в дальнейшем при изучении таких дисциплин как: «Сети и системы передачи информации»; «Программно-аппаратные средства обеспечения информационной безопасности»; «Модели безопасности компьютерных систем».

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

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- способностью анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач (ОПК-1);

- способностью применять нормативные правовые акты в профессиональной деятельности (ОПК-6);
- способностью проводитьанализ защищенности автоматизированных систем (ПК-3);
- способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);
- способностью проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);
- способностью участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);
- способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);
- способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем (ПК-15);
- способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);
- способностью проводить инструментальный мониторинг защищенности информации вавтоматизированной системе и выявлять каналы утечки информации (ПК-17).

В результате изучения дисциплины студент должен:

- **знать:**

основы физической защиты объектовинформатизации;
технические каналы утечки информации;
основные нормативные правовые акты в профессиональной деятельности;
возможности технических средств перехвата информации;
организацию защиты информации от утечки по техническим каналам на объектах информатизации;
основные операции контрольных проверок работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации;
способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;

- **уметь:**

пользоваться нормативными документами по противодействию технической разведке;
анализировать и оценивать угрозы информационной безопасности объекта;
анализировать физические явления и процессы, применять соответствующий математический аппарат для формализации и решения профессиональных задач;
проводить анализ защищенности автоматизированных систем;
проводить контрольные проверки работоспособности применяемых технических средств защиты;
проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации;

владеть:

математическим аппаратом для формализации и решения профессиональных задач;
методологией оценки рисков;
методами и средствами технической защиты информации;
методами расчета и инструментального контроля показателей технической защиты

информации.

4. ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ

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

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 технологииразвивающего, проблемного и проектного обучения.

6. КОНТРОЛЬ УСПЕВАЕМОСТИ

Программой дисциплины предусмотрены следующие виды текущего контроля: письменные и устные опросы на лекциях, написание рефератов.

Промежуточная аттестация проводится в форме экзамена.