АННОТАЦИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

«Техническая защита информации»

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» изучается в 6 семестре и относится к базовой части дисциплин блока Б1.Б специальности 10.05.03 «Информационная безопасность автоматизированных систем».

Курс учебной дисциплины тесно связан с другими учебными дисциплинами, позволяющими понять физическую сущность возникновения технических каналов утечки информации, возможности современных средств технической разведки, методы и способы защиты от утечки по техническим каналам.

3. Требования к результатам освоения дисциплины

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 проводить анализ 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 требований по защите информации (ПК-16);

способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

В результате изучения дисциплины студент должен:

- **знать:**

организацию защиты информации от утечки по техническим каналам на объектах информатизации;

способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации;

технические каналы утечки информации;

возможности технических средств перехвата информации;

- **уметь:**

пользоваться нормативными документами по противодействию технической разведке;

использовать типовые приборы для выявления и защиты основных каналов утечки информации;

- **владеть**:

методами и средствами технической защиты информации;

методами расчета и инструментального контроля основных показателей технической защиты информации.

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: семинарские и лабораторные занятия, интерактивный опрос, эвристическая беседа, диалог, ознакомительные беседы с представителями потенциальных работодателей.

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

6. Контроль успеваемости

Программой дисциплины предусмотрены следующие виды текущего контроля: письменные и устные опросы на семинарских занятиях, опрос во время лекций, написание рефератов.

Промежуточная аттестация проводится в форме экзамена.