

**Аннотация к рабочей программе**  
**дисциплины «Техническая защита информации»**  
**специальность 10.05.03 «Информационная безопасность АС»**  
**(специализация «Информационная безопасность АС на транспорте»).**

**Общая трудоемкость дисциплины** составляет 4 зачетных единиц.

**Форма контроля:** зачет 8 семестр, экзамен 9 семестр

Предполагаемые семестры: 8,9.

**Целью** изучения дисциплины (модуля) является подготовка выпускников к деятельности, связанной с разработкой, внедрением и эксплуатацией инженерно-технических методов и средств защиты информации в автоматизированных системах управления и обработки информации.

**Задачами** курса являются:

- изучение технических каналов утечки информации и возможностей технических разведок;
- изучение способов и средств защиты информации от утечки по техническим каналам;
- освоение методов и средств контроля эффективности технической защиты информации.

**Дисциплина относится к профессиональному циклу (вариативная часть).** Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- математический анализ;
- информатика;
- физика;
- основы информационной безопасности;
- электроника и схемотехника;
- организация ЭВМ и вычислительных сетей.

**Краткое содержание дисциплины:**

Предмет и задачи технической защиты информации. Направления технической защиты информации.

Теоретические основы инженерно-технической защиты информации. (в т.ч. источники опасных сигналов, технические каналы утечки информации)

Физические основы инженерно-технической защиты информации

Технические средства добывания и защиты информации

Организационные основы инженерно-технической защиты информации

Методическое обеспечение инженерно-технической защиты информации

Выпускник должен обладать следующими **профессиональными компетенциями (ПК):**

ПК-12: способностью участвовать в разработке подсистем управления информационной безопасностью;

ПК-13: способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности;

ПК-14: способностью проводить анализ рисков информационной безопасности автоматизированной системы;

ПК-15: способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем;

ПК-16: способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ;

Специализация № 10 «Информационная безопасность автоматизированных систем на транспорте»:

ПСК-10.8: способностью осуществлять рациональный выбор элементной базы обеспечения информационной безопасности распределенных автоматизированных, информационно-управляющих и информационно-логистических систем транспорта.

В результате изучения дисциплины специалист должен:

**Знать:**

- виды, источники и носители защищаемой информации;
- основные угрозы безопасности информации;
- концепцию инженерно-технической защиты информации;
- основные принципы и методы инженерно-технической защиты информации;
- основные руководящие и нормативные документы по инженерно-технической защите информации;
- порядок организации инженерно-технической защиты информации;

**Уметь:**

- выявлять угрозы и технические каналы утечки информации;
- описывать (моделировать) объекты защиты и угрозы безопасности информации;
- применять наиболее эффективные методы и средства инженерно-технической защиты информации;
- контролировать эффективность инженерно-технических мер защиты;

**Владеть:**

- профессиональной терминологией;
- методами инженерного расчета размеров контролируемой зоны;
- навыками внедрения и эксплуатации современных средств инженерно-технической защиты информации.