

Аннотация к рабочей программе дисциплины «Техническая защита информации»

Рабочая программа дисциплины «Техническая защита информации» разработана для студентов направления «Информационная безопасность».

Целью дисциплины является теоретическая и практическая подготовленность бакалавра к организации и проведению мероприятий по защите информации от утечки по техническим каналам на объектах информатизации и в выделенных помещениях.

Задачами дисциплины являются:

- ознакомление с техническими каналами утечки информации, обрабатываемой средствами вычислительной техники и автоматизированными системами;
- ознакомление с техническими каналами утечки акустической (речевой) информации;
- изучение способов и средств защиты информации, обрабатываемой техническими средствами;
- изучение способов и средств защиты выделенных (защищаемых) помещений от утечки акустической (речевой) информации;
- изучение методов и средств контроля эффективности защиты информации от утечки по техническим каналам;
- обучение основам организации технической защиты информации на объектах информатизации и в выделенных помещениях.

В результате изучения данной дисциплины у обучающихся формируются следующие профессиональные компетенции.

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-7) способностью определять информационные ресурсы, подлежащие защите,	Знает	возможные нестандартные ситуации
	Умеет	принимать решения и нести ответственность
	Владеет	навыками и умениями принимать решения в

угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты		нестандартных ситуациях
(ПК-3) способностью администрировать подсистемы информационной безопасности объекта защиты	Знает	вероятные угрозы и уровни развития технологий защиты информации
	Умеет	организовывать и поддерживать выполнение комплекса мер по информационной безопасности
	Владеет	навыками управления процессом защиты с учетом решаемых задач и организационной структуры объекта защиты
(ПК-8) способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	Знает	основы информационной безопасности
	Умеет	принимать участие в эксплуатации подсистем управления информационной безопасностью
	Владеет	навыками применения мер по защите информации