Аннотация
к рабочей программе дисциплины
«Противодействие техническим разведкам»

по направлению 10.03.01 «Информационная безопасность»
(профиль «Безопасность автоматизированных систем»)

Общая трудоемкость дисциплины составляет 3 зачетных единиц.(108 часов)

Форма контроля: зачет 6 семестр.

Предполагаемые семестры: 6

Цель «Противодействие техническим разведкам» приобрести теоретические знания и навыки работы, необходимые для защиты информационных ресурсов организации от приемов конкурентов, направленных на изъятие с помощью технических.

Задачи курса:

В результате изучения дисциплины бакалавр должен:

Знать, технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации, принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации. Уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты, анализировать и оценивать угрозы информационной безопасности объекта. Владеть методами и средствами выявления угроз безопасности АС, методами технической защиты информации.

Учебная дисциплина

Дисциплина является самостоятельным элементом в системе подготовки специалиста, относится к циклу Б1.В.ДВ. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- основы информационной безопасности;
- сети, системы передачи информации
- информатика.

В дисциплине «Противодействие техническим разведкам» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- технология построения защищенных автоматизированных систем;
- комплексное обеспечение информационной безопасности АС;
- интегрированные информационные системы в управлении.

Краткое содержание дисциплины:

Механизмы и технологии технической разведки, основные направления противодействия техническим средствам разведки, физические и технические основы противодействия техническим средствам разведки, технический (инструментальный) контроль защиты информации, служба безопасности современного российского предприятия.

В результате изучения дисциплины, специалист должен обладать следующими профессиональными компетенциями (ПК):

ПК-1: способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;

ПК-2: способность принимать участие в эксплуатации подсистем управления информационной безопасностью объекта защиты;

ПК-17: способность изучать и обобщать опыт работы различных учреждений, организаций и предприятий в области повышения эффективности защиты информации.

В результате изучения дисциплины бакалавр должен:

Знать:

- технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации;
- принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.

Уметь:

- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- анализировать и оценивать угрозы информационной безопасности объекта.

Владеть:

- методами и средствами выявления угроз безопасности автоматизированным системам;
- методами технической защиты информации.