Аннотация рабочей программы дисциплины (модуля)

Б1.В.ДВ.09.01 Основы информационной безопасности

Цели дисциплины

Целями дисциплины являются изучение принципов информационной безопасности предприятия, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации; освоения основ их комплексного построения на различных уровнях защиты и особенностей степеней защиты для государственного и частного назначения.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

- изучение основных принципов информационной безопасности предприятия;
- ознакомление с техническими и технологическими решениями, используемыми в данной области;
- выработка практических навыков аналитического и экспериментального исследования основных методов и средств, используемых в области, изучаемой в рамках данной дисциплины.

Формируемые компетенции и индикаторы их достижения по дисциплине

Коды компетенции	Содержание компетенций	Код и наименование индикатора достижения компетенции
ПКС-1	Способен разрабатывать, изменять и согласовывать архитектуры программного обеспечения с системным аналитиком и архитектором программного обеспечения	ПКС-1.1 Знать существующие архитектуры программного обеспечения. ПКС -1.2 Уметь использовать существующие архитектуры программного обеспечения. ПКС-1.3 Иметь навыки разработки и программного обеспечения различных архитектур.
ПКС-4	Способен проектировать программные интерфейсы	ПКС-4.1 Знать основные принципы проектирования программных интерфейсов. ПКС -4.2 Уметь использовать принципы проектирования программных интерфейсов. ПКС-4.3 Иметь навыки проектирования программных интерфейсов.

Содержание разделов дисциплины

7 семестр

Тема 1. Информационная безопасность в системе национальной безопасности Российской Федерации

Понятие информационной безопасности. Национальные интересы Российской Федерации в информационной сфере и их обеспечение. Виды угроз информационной безопасности Российской Федерации. Источники угроз информационной безопасности Российской Федерации. Информационная безопасность и информационное противоборство.

Тема 2. Обеспечение информационной безопасности объектов информационной сферы государства в условиях информационной войны

Основные направления обеспечения информационной безопасности объектов информационной сферы государства. Общие методы обеспечения информационной безопасности Российской Федерации. Методы и средства обеспечения безопасности компьютерных систем.

Тема 3. Общая характеристика КЗИ

Комплексная защита информации - сущность и задачи Стратегии комплексной защиты информации, стадии их создания Структура, характеристики принципы построения и этапы разработки комплексной защиты информации объекта.

Тема 4. Конфиденциальный документ

Критерии ценности информации и направления ее формирования. Выявление конфиденциальных сведений. Перечень конфиденциальных сведений. Носители конфиденциальных данных. Конфиденциальные документы: состав, сроки, реквизиты. Угрозы конфиденциальному документу. Жизненный цикл открытого и конфиденциального документа. Документированная система защиты информации.

Тема 5. Испытание программного и аппаратного уровней КЗИ

Тестовые испытания программных средств защиты. Анализ сетевой топологии и установленных сервисов. Сетевое сканирование. Анализ трафика и сбор критичной информации программами пассивного анализа. Обнаружение уязвимостей по сигнатурам.

Тема 6. Система физической защиты в КЗИ

Система физической защиты - типовые задачи и способы ее реализации. Связь между функциями и основные характеристики системы физической защиты. Принципы обеспечения эффективности системы физической защиты, путь и стратегии нарушителя. Количественный и качественный анализ системы физической защиты. Диаграмма последовательности действий нарушителя. Применение технических, инженерных средств и сооружений охраны. Силы реагирования системы физической защиты, основные принципы их организации.

Тема 7. Организация и аудит КЗИ

Жизненный цикл организации работ по комплексной защите информации на объекте. Система анализа угроз и рисков комплексной защиты информации на объекте «Гриф». Система анализа и управления политикой информационной безопасности на объекте «Кондор» ISO 17799. Содержание и последовательность работ по комплексной защите информации на объекте ГОСТ 15408.