

Аннотация рабочей программы дисциплины (модуля)
Б1.В.08 «Основы информационной безопасности»

Цель дисциплины

Целью дисциплины является изучение принципов обеспечения информационной безопасности государства и организаций, подходов к анализу угроз его информационной инфраструктуры и освоение дисциплинарных компетенций для решения задач защиты информации в информационных системах, а также формирование фундаментальных знаний в области информационной безопасности.

Задачи дисциплины

- изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации;
- изучение видов защищаемой информации, угроз информационной безопасности, сущности и разновидностей информационного оружия, методов и средств ведения информационных войн;
- изучение методов и средств обеспечения информационной безопасности компьютерных систем, механизмов защиты информации, формальных моделей безопасности, критериев оценки защищенности и обеспечения безопасности автоматизированных систем;
- приобретение умений в подборе и анализе показателей качества и критериев оценки систем безопасности, отдельных методов и средств защиты информации, использовании современной научно-технической литературой для решения задач по вопросам защиты информации;
- приобретение навыков анализа информационной инфраструктуры государства с точки зрения информационной безопасности, подбора нормативных и методических материалов по вопросам защиты информации.

Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	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

Содержание разделов дисциплины

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. Общие методы обеспечения информационной безопасности Российской Федерации. Методы и средства обеспечения

безопасности компьютерных систем. Основные направления обеспечения информационной безопасности объектов информационной сферы государства.

Тема 2. Классификация информации, подлежащей защите в соответствии с законодательством Российской Федерации. Государственная тайна. Государственная система защиты информации.

Информация как объект правовых отношений. Общедоступная информация. Информация ограниченного доступа. Конфиденциальная информация: коммерческая тайна; служебная тайна; профессиональная тайна; личная тайна; семейная тайна; персональные данные. Государственная тайна.

Тема 3. Методологические основы защиты информации

Методы и технологии защиты информации. Классификация методов и средств защиты информации. Антивирусная защита. Системы идентификации и аутентификации. Системы разграничения доступа. Стенографические и криптографические методы. Технология электронной подписи. Методы обнаружения и блокирования угроз информационной безопасности. Методы защиты в операционных системах. Сетевые технологии защиты.

Тема 4. Угрозы информационной безопасности

Анализ уязвимостей системы. Классификация угроз информационной безопасности. Основные направления и методы реализации угроз. Неформальная модель нарушителя. Оценка уязвимости системы.

Тема 5. Построение систем защиты информации

Определение и основные способы несанкционированного доступа. Методы защиты от несанкционированного доступа: организационные методы защиты; инженерно-технические методы защиты; построение систем защиты от угрозы утечки по техническим каналам. Идентификация и аутентификация. Использование криптографических методов. Защита целостности информации при хранении; обработке; транспортировке. Построение систем защиты от угрозы отказа доступа к информации.

Тема 6. Нормативно правовое регулирование защиты информации

Нормативно-правовые документы в области информационной безопасности в РФ. Законодательные акты в области защиты информации. Российские и международные стандарты, определяющие требования к защите информации. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации.