

Аннотация рабочей программы дисциплины (модуля) Б1.В.ДВ.05.01 Прикладная криптография

Цели дисциплины

Целями освоения дисциплины Прикладная криптография является формирование профессиональных компетенций будущих специалистов в области Информационных систем и технологий, представлений о практическом использовании криптографических методов защиты информации для решения отдельных задач обеспечения информационной безопасности.

Задачи дисциплины

Основными задачами изучения дисциплины являются:

- формирование представления об основных проблемах, связанных с практическим использованием криптографических методов защиты информации.
- изучение основных криптографических протоколов.
- изучение инфраструктуры открытого ключа.
- изучение механизмов управления ключами.

Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС-1	Способен проводить формализацию предметной области с целью создания информационной системы в сфере профессиональной деятельности	ПКС-1.1 - Знает критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем; ПКС-1.2 - Умеет определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы; ПКС-1.3 – Владеет навыками определения параметров настройки программного обеспечения системы защиты информации автоматизированной системы;

Содержание разделов дисциплины

Тема 1. Введение в прикладные аспекты криптографической защиты информации

Понятие криптографического протокола. Роль криптографических протоколов в системах защиты информации. Основные атаки на криптографические протоколы. Протоколы идентификации на основе паролей, протоколы «рукопожатия» и типа «запрос-ответ». Понятие протоколов интерактивного доказательства и доказательства знания. Протоколы идентификации на основе протоколов доказательства знания с нулевым разглашением.

Тема 2. Инфраструктура открытых ключей

Основные компоненты инфраструктуры открытых ключей. Понятие сертификата открытого ключа. Удостоверяющий центр. Архитектура инфраструктуры открытого ключа.

Тема 3. Механизмы управления ключами

Изучение стандарта ISO/IEC 11770. Механизмы, использующие симметричные методы. Механизмы, использующие асимметричные методы. Механизмы, основанные на слабых секретах. Управление групповыми ключами. Формирование ключей.

Тема 4. Практические аспекты криптографической защиты информации

Проблемы реализации криптографических алгоритмов. Защита от утечки информации. Построение безопасного коммуникационного канала на основе криптографических алгоритмов.