

ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

27.03.02 – Управление качеством

Аннотация рабочей программы

дисциплины «Информационные технологии в управлении качеством и защита информации»

Общая трудоемкость дисциплины составляет 4 зач. единицы, 144 часа, форма промежуточной аттестации – зачет.

Программой дисциплины предусмотрены лекционные (34 часа), практические (34 часа), самостоятельная работа обучающегося составляет 76 часов

В результате освоения дисциплины обучающийся должен:

- ▲ Знать: информационные технологии, применяемые в области управления качеством, методы и средства обеспечения защиты информации.
- ▲ Уметь: разрабатывать модели и алгоритмы процессов.
- ▲ Владеть: навыками защиты информации.

Дисциплина предусматривает изучение следующих основных разделов:

1. Информационные технологии в управлении качеством. Разработка моделей и алгоритмов процессов бизнеса. Информационная модель фирмы и агентские отношения. Понятия теории информации. Защищаемая информация. Факторы, воздействующие на информацию, объекты информатизации. Классы информационных ресурсов. Информационные системы. Информационные технологии. Модель информационно-технологического цикла управления качеством. Теория принятия решений. Методы принятия решений в условиях неопределенности. Структура системы организационного управления качеством.

2. Экспертные системы в управлении качеством. Общая характеристика экспертных систем. Структура и использование экспертных систем. Классификация инструментальных средств экспертных систем. Организация знаний в экспертных системах. Отличия экспертных систем от традиционных программ. Виды экспертных систем. Типы задач в управлении качеством, решаемых экспертными системами.

3. Защита информации. Методы формирования функции защиты. Классы задач защиты информации. Состояния и функции системы защиты. Стратегия защиты информации. Способы и средства защиты информации. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Введение и общая модель. Функциональные компоненты безопасности. Аудит безопасности. Криптографическая поддержка. Защита данных пользователя. Идентификация и аутентификация.

4. Международные стандарты на системы управления информационной безопасностью. Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Практические правила управления информационной безопасностью. Руководство по внедрению системы управления информационной безопасностью. Управление рисками информационной безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью.