Аннотация дисциплины Б1.В.ДВ.3.2 – «Безопасность информационных систем»

Общая трудоемкость изучения дисциплины составляет 3 ЗЕТ (108 час.)

Цели и задачи дисциплины: цель – формирование у студента способности использовать современные технологии обработки информации, современные технические средства управления, вычислительную технику, технологии компьютерных сетей и телекоммуникаций при проектировании систем автоматизации и управления с учетом безопасности информационных данных; задачи - изучение основ информационной деятельности предприятия; изучение международных и отечественных правовых и нормативных актов обеспечения информационной безопасности; освоение методов защиты технических средств и объектов предприятий от утечки информации и несанкционированного доступа; умение использовать методы и средства парирования и нейтрализации информационных угроз; обеспечение информационной безопасности в типовых ОС, СУБД, вычислительных сетях и в Интернете; устранение последствия информационных атак.

Компетенции обучающегося, формируемые в результате освоения дисциплины: ПК-2 способность применять современные теоретические и экспериментальные методы разработки математических моделей исследуемых объектов и процессов, относящихся к профессиональной деятельности по направлению подготовки ; ПК-3 способность применять современные методы разработки технического, информационного и алгоритмического обеспечения систем автоматизации и управления; ПК-10 способность использовать современные технологии обработки информации, современные технические средства управления, вычислительную технику, технологии компьютерных сетей и телекоммуникаций при проектировании систем автоматизации и управления.

В результате изучения дисциплины студент должен:

знать: методологии создания систем защиты информации; основные функции, назначение составных частей и принципы построения систем компьютерной безопасности; проблемы построения систем зашиты информации (СЗИ) и организации её функционирования, а также об основных направлениях решения этих проблем и направлениях дальнейшего развития; методики проведения сравнительного анализа систем защиты информации; основы менеджмента современных систем информационной безопасности (ПК-10);

уметь: квалифицированно оценивать область применения элементов СЗИ; грамотно использовать элементы СЗИ при решении практических задач; использовать все возможности, предоставляемые системой защиты; адекватно управлять системой информационной безопасности (ПК-2);

владеть: навыками освоения и внедрения новых систем комплексной защиты информации; навыками сопровождения и управления системами КЗИ; аппаратом исследования различных систем КЗИ (ПК-3).

Содержание дисциплины: Основные понятия информационной безопасности. Проблемы информационной безопасности сетей. Политика безопасности. Криптографическая зашита информации. Идентификация, аутентификация и управление доступом. Защита электронного документооборота. Принципы комплексной защиты информационных систем. Безопасность операционных систем. Протоколы защищенных каналов. Межсетевое экранирование. Виртуальные защищенные сети VPN. Защита удаленного доступа. Обнаружение и предотвращение вторжений. Защита от вредоносных программ, сетевых атак, баннер и спама. Управление средствами обеспечения информационной безопасности. Стандарты информационной безопасности.

Форма итогового контроля по дисциплине: зачет, курсовой проект.