АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ
Администрирование и безопасность информационных систем

Направление подготовки: **09.03.04 «Программная инженерия»**
Профиль подготовки: **Разработка программно-информационных систем**
Уровень высшего образования: **бакалавриат**
Форма обучения: **очная**

Цели освоения дисциплины

Целью освоения дисциплины является овладение студентами теоретических и практических основ администрирования информационных систем; способов управления информационными сетями, администрирования операционных систем, приложений, сетевых и информационных сервисов, баз данных. Также формирование у студентов специальных знаний в области управления современными системами информационной безопасности и защиты информации.

Планируемые результаты освоения дисциплины

В результате освоения дисциплины обучающиеся должны обладать следующими общекультурными и общепрофессиональными компетенциями:

– способностью использовать основы правовых знаний в различных сферах жизнедеятельности (ОК-4);

– владением архитектурой электронных вычислительных машин и систем (ОПК-2);

– способностью осуществлять поиск, хранение, обработку и анализ информации из различных источников и баз данных, представлять ее в требуемом формате с использованием информационных, компьютерных и сетевых технологий (ОПК-4).

В результате освоения дисциплины обучающийся должен демонстрировать следующие результаты образования:

1. Знать: основные понятия администрирования информационных систем; основные задачи администратора операционной системы и доступный для управления операционной системой инструментарий; основные задачи администратора сервера баз данных и доступный для управления сервером баз данных инструментарий; структуру основных служб администрирования; принципы построения и организацию функционирования вычислительных сетей, их функциональную и структурную организацию; основные понятия информационной безопасности и направления защиты информации; стандарты информационной безопасности распределенных систем и анализ угроз; механизмы обеспечения информационной безопасности; принципы построения и направления работ по созданию систем информационной безопасности и методологии защиты информации (ОК-4, ОПК-2, ОПК-4).

2. Уметь: проводить инсталляцию, конфигурирование и загрузку операционных систем, в том числе сетевых; диагностировать и восстанавливать операционные системы при сбоях и отказах; использовать программные средства мониторинга операционных средств и утилиты сетевых протоколов в интересах эффективности и оптимизации операционных систем; производить конфигурирование ролей контроллера домена и его объектов; управлять пользователями домена и сервера баз данных; используя инструментальные средства операционной системы, управлять пользователями; конфигурировать аппаратные и программные средства системы; обеспечить протоколирование и аудит ИС, контроль и управление доступом, контроль целостности; проводить оценку угроз безопасности объекта информатизации; реализовывать простые информационные технологии, реализующие методы защиты информации (ОК-4, ОПК-2, ОПК-4).

3. Владеть: специальной терминологией, основами администрирования и безопасности информационных систем; конфигурированием, отладки, и обслуживанием основных служб корпоративной компьютерной сети; приемами работы в интегрированной среде

администрирования Microsoft server 2012; методами и инструментальными средствами защиты информации; навыками программирования алгоритмов криптографической защиты информации (ОК-4, ОПК-2, ОПК-4).

Основное содержание дисциплины

Основные понятия администрирования и безопасности информационных систем.

Операционные системы.

Базовые средства администрирования Windows 2012 Server. Управление доменом. Active Directory.

Механизм групповой политики, файловый сервер, служба DFS.

Методы и технологии защиты информационных систем. Модель построения корпоративной системы защиты информации.

Основные виды угроза безопасности ИС и информации. Криптография, классификации крипто алгоритмов. Основы криптографии.

Системы резервного копирования и восстановления данных. Эффективность информационных систем.

Вредоносные программы и их классификация. Антивирусы. Принцип работы. Алгоритмы обнаружения вредоносных ПО.

Межсетевой экран. Система обнаружения вторжений. Механизм работы файерволла.