Аннотация к рабочей программе дисциплины «Безопасность сетей ЭВМ»

по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация «Информационная безопасность АС на транспорте»).

Общая трудоемкость дисциплины составляет 8 зачетных единиц (288 часов).

Предполагаемые семестры: 7,8

Форма контроля: зачет -7 семестр, курсовая работа, экзамен - 8 семестр

Целью изучения дисциплины (модуля) является обучение студентов основам построения и эксплуатации вычислительных сетей, принципам и методам защиты информации в компьютерных сетях, навыкам комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей.

Задачами курса являются изучение основ архитектуры вычислительных сетей, их эксплуатации и обеспечение их безопасности, которые включают в себя все методы и средства обеспечения безопасности вычислительных сетей:

Дисциплина относится к циклу Б1. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин: Высшая математика, Физика, Основы информационной безопасности, Системы и сети передачи данных, Безопасность операционных систем.

Дисциплина *«Безопасность сетей ЭВМ»* необходима для изучения курса «Комплексное обеспечение информационной безопасности автоматизированных систем».

Краткое содержание дисциплины:

Перспективные направления развития технологий обеспечения безопасности в сетях. Роль и место защиты информации в сетях при решении задач, связанных с обеспечением комплексной ИБ.

Методологические и технологические основы обеспечения ИБ сетевых автоматизированных систем.

Угрозы и методы нарушения ИБ сетевых АС. Типовые модели атак, направленные на преодоление защиты сетевых АС, условия их осуществимости, возможные последствия, способы предотвращения. Роль человеческого фактора в обеспечении безопасности сетей. Возможности, способы и правила применения основных программных и аппаратных средств защиты информации в сетях. Принципы функционирования основных защищенных сетевых протоколов. Основы применения межсетевых экранов для защиты сетей. Правила определение политики сетевой безопасности. Стандарты по оценке защищенных сетевых систем и их теоретические основы. Методы и средства проектирования, реализации и оценки защищенных сетевых систем.

В результате изучения дисциплины бакалавр должен обладать следующими компетенциями:

ПК-4: способностью проводить анализ защищенности автоматизированных систем.

ПК-5: способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы.

ПК-6: способностью проводить анализ рисков информационной безопасности автоматизированной системы.

ПК-7: способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем.

ПК-8: способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ.

В результате изучения дисциплины бакалавр должен:

Знать:

- принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей;
- основные протоколы компьютерных сетей;
- последовательность и содержание этапов построения компьютерных сетей;
- эталонную модель взаимодействия открытых систем;
- основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях.

Уметь:

- проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети;
- эффективно использовать различные методы и средства защиты информации для компьютерных сетей;
- проводить мониторинг угроз безопасности компьютерных сетей.

Владеть:

- навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности;
- навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности;
- навыками использования программно-аппаратных средств обеспечения безопасности компьютерных сетей;
- методиками оценки показателей качества и эффективности ЭВМ и вычислительных систем.

.