Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Саратовский государственный технический университет имени Гагарина Ю.А.»

Кафедра «Информационная безопасность автоматизированных систем»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ

по дисциплине

«Б.1.1.30 Безопасность сетей ЭВМ»

направления подготовки
10.03.01 "Информационная безопасность"
Профиль "Безопасность автоматизированных систем"

форма обучения – очная
курс – 3
семестр – 6
зачетных единиц – 5
часов в неделю – 4
всего часов – 180,
в том числе:
лекции – 32
практические занятия – 32
самостоятельная работа – 116
экзамен – 6 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: 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, а также содействовать фундаментализации образования, формированию научного мировоззрения и развитию системного мышления. Дисциплина является базовой для изучения дисциплин по комплексному и организационному обеспечению информационной безопасности.

Задачи изучения дисциплины:

- изучение архитектуры вычислительных сетей;
- изучение программно-аппаратных и технических средств создания сетей;
- изучение принципов построения сетей и управления ими;
- изучение правил организационной, технической и правовой защиты;
- изучение основ использования программных и аппаратных технологий защиты сетей;
- изучение методологии проектирования, развертывания и сопровождения безопасных сетей;
- знакомство с методологией обследования и анализа защищенных вычислительных сетей.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Безопасность сетей ЭВМ» относится к базовой части дисциплин.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Информатика» – знать формы и способы представления данных в персональном компьютере, типовые структуры и принципы организации компьютерных сетей;

«Языки программирования» – знать язык программирования высокого уровня (объектно-ориентированное программирование), уметь работать с интегрированной средой разработки программного обеспечения, владеть навыками разработки, документирования, тестирования и отладки программного обеспечения в соответствии с современными технологиями и методами программирования;

«Основы информационной безопасности» – знать сущность и понятие информации, информационной безопасности и характеристику ее составляющих, источники и классификацию угроз информационной безопасности, основные средства и способы обеспечения информационной безопасности, принципы

построения систем защиты информации, владеть профессиональной терминологией в области информационной безопасности;

«Сети и системы передачи информации» – знать основные характеристики сигналов электросвязи, спектры и виды модуляции, принципы построения и функционирования систем и сетей передачи информации, способы кодирования информации, основные телекоммуникационные протоколы.

Дисциплина «Безопасность сетей ЭВМ» является предшествующей для изучения следующих базовых дисциплин: «Управление информационной безопасностью», «Программно-аппаратные средства обеспечения информационной безопасности», «Безопасность защищенных вычислительных сетей».

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

- способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);
- способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7).

Студент должен знать:

- принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей;
- эталонную модель взаимодействия открытых систем, методы коммутации и маршрутизации, сетевые протоколы;
- последовательность и содержание этапов построения компьютерных сетей;
- основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в компьютерных сетях;
- основы администрирования вычислительных сетей;
- принципы организации информационных систем в соответствии с требованиями по защите информации;
- методологические и технологические основы обеспечения информационной безопасности сетевых автоматизированных систем;
- угрозы и методы нарушения информационной безопасности сетевых автоматизированных систем;
- типовые модели атак, направленных на преодоление защиты сетевых автоматизированных систем, 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 определения политики сетевой безопасности;
- основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю в данной области;
- методы, способы, средства, последовательность и содержание этапов разработки автоматизированных систем и подсистем безопасности автоматизированных систем;
- автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности;
- содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и подсистем безопасности автоматизированных систем;
- принципы формирования политики информационной безопасности в автоматизированных системах.

Студент должен уметь:

- проводить анализ сетевых автоматизированных систем с точки зрения обеспечения информационной безопасности;
- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- проектировать и администрировать компьютерные сети, реализовывать политику безопасности компьютерной сети;
- применять защищенные протоколы и межсетевые экраны, необходимые для реализации систем защиты информации в сетях;
- реализовывать меры противодействия выявленным угрозам сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения;
- пользоваться нормативными документами по защите информации;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- разрабатывать частные политики информационной безопасности автоматизированных систем;
- формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;
- разрабатывать проекты нормативных и организационно- распорядительных документов, регламентирующих работу по защите информации;

Студент должен владеть:

- профессиональной терминологией в области информационной безопасности;
- навыками эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) 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 защиты сетей;
- методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений;
- навыками комплексного анализа и оценки сетевой безопасности;
- навыками работы с нормативными правовыми актами;
- навыками организации и обеспечения режима секретности;
- методами организации и управления деятельностью служб защиты информации на предприятии;
- навыками безопасного использования технических средств в профессиональной деятельности.