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

«С.1.1.20 Безопасность сетей ЭВМ»

специальности подготовки
10.05.03 "Информационная безопасность автоматизированных систем"
Специализация №9 "Создание автоматизированных систем в защищенном исполнении"

форма обучения – очная
курс – 4
семестр – 7
зачетных единиц – 5
часов в неделю – 4
всего часов – 180,
в том числе:
лекции – 32
практические занятия – 32
самостоятельная работа – 116
экзамен – 7 семестр
курсовая работа – 7 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 к базовой части блока 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 проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24).

Студент должен знать:

- место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;
- терминологию, основные руководящие и регламентирующие документы в области ЭВМ, комплексов и систем;
- основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;
- 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;
- 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;

Студент должен уметь:

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности;
- 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;
- проводить анализ сетевых автоматизированных систем с точки зрения обеспечения информационной безопасности;
- разрабатывать модели и политику сетевой безопасности, используя известные подходы, методы, средства и теоретические основы;
- применять стандарты по оценке защищенных сетевых систем при анализе и проектировании систем защиты информации в автоматизированных системах;
- 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;
- реализовывать системы защиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем.

Студент должен владеть:

- профессиональной терминологией в области информационной безопасности;
- навыками работы с нормативными правовыми актами;
- навыками, эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) локальных компьютерных сетей с учетом требований по обеспечению информационной безопасности;
- навыками разработки, документирования компьютерных сетей с учетом требований по обеспечению безопасности;

- навыками использования программно-аппаратных средств обеспечения сетей;
- навыками построения и эксплуатации вычислительных сетей;
- навыками комплексного анализа и оценки сетевой безопасности.