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.1.2.7. Безопасность защищенных вычислительных сетей»

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

форма обучения – очная
курс – 4
семестр – 8
зачетных единиц – 5
часов в неделю – 5
всего часов – 180,
в том числе:
лекции – 32
практические занятия – 48
самостоятельная работа – 100
экзамен – 8 семестр
зачет – 8 семестр

1. Цели и задачи дисциплины

Цель преподавания дисциплины: теоретическая и практическая подготовка специалистов в области построения защищенных вычислительных сетей.

Задачи изучения дисциплины:

- изучение основных элементов теории построения защищенных вычислительных сетей;
- изучение основных принципов функционирования средств защиты сетей;
- привитие навыков комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей;
- изучение основных угроз в сетях ЭВМ и методов противодействия им;
- овладение механизмами построения защищенных вычислительных сетей.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Безопасность защищенных вычислительных сетей» относится к вариативной 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 защищенных вычислительных сетей» является предшествующей для изучения следующих базовых дисциплин: «Управление

информационной безопасностью», «Программно-аппаратные средства обеспечения информационной безопасности», «Создание автоматизированных систем в защищенном исполнении».

3. Требования к результатам освоения дисциплины

Изучение дисциплины направлено на формирование следующих компетенций:

способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);

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

Студент должен знать:

- основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации;
- организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации;
- принципы построения и функционирования, примеры реализаций современных локальных и глобальных компьютерных сетей;
- последовательность и содержание этапов построения компьютерных сетей;
- эталонную модель взаимодействия открытых систем;
- основные криптографические методы, алгоритмы, протоколы, используемые для обеспечения безопасности в сетях ЭВМ;

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;
- разрабатывать технические задания на создание подсистем информационной безопасности автоматизированных систем, проектировать такие подсистемы с учетом действующих нормативных и методических документов;
- 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;

Студент должен владеть:

- профессиональной терминологией в области информационной безопасности;
- навыками работы с нормативными правовыми актами;
- методами формирования требований по защите информации;
- 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 сетей ЭВМ: межсетевых экранов, систем VPN, систем обнаружения атак, систем-ловушек, сканеров безопасности для защиты сетей.