Аннотация

к рабочей программе дисциплины

Б1.В.ОД.8. «Технология построения защищенных автоматизированных систем»

по направлению 10.03.01 «Информационная безопасность»

(профиль «Безопасность автоматизированных систем»)

Общая трудоемкость дисциплины составляет 5 зачетных единиц.(180 часов)

Форма контроля: курсовая работа, экзамен 7 семестр.

Предполагаемые семестры: 7

Цель

- получении знаний и навыков работы, необходимых для разработки и эксплуатации автоматизированных систем, информационные ресурсы которых содержат конфиденциальную информация.
- решении задач, требующих классификации и структуризации мер обеспечения безопасности АС от степени конфиденциальности.

Задачи курса: изучить

- принципы построения информационных систем;
- принципы организации информационных систем в соответствии с требованиями по защите информации;
- основные нормативные правовые акты в области информационной безопасности и защиты, а также нормативные методические документы ФСБ РФ;
- меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- угрозы информационной безопасности объекта;
- отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
- методы и средства выявления угроз безопасности АС; методы технической защиты информации.

Приобрести навыки организации и обеспечения режима секретности.

Учебная дисциплина

Дисциплина является самостоятельным элементом в системе подготовки специалиста, относится к циклу Б3.В4. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- основы информационной безопасности;
- принципы построения, проектирования и эксплуатации автоматизированных информационных систем;
- информационная безопасность открытых систем.

В дисциплине «Технология построения защищенных автоматизированных систем» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:

- комплексное обеспечение информационной безопасности автоматизированных систем
- интегрированные информационные системы в управлении.

Краткое содержание дисциплины:

Нормативно-методическая база создания защищенных автоматизированных систем (ЗАС), стадии и этапы создания ЗАС и требования по защите информации, синтез программно-аппаратных средств ЗАС, методы, способы и средства обеспечения отказоустойчивости ЗАС, структура подсистем защиты информации от несанкционированного доступа (НСД), оценка защищенности на этапах жизненного цикла ЗАС, мониторинг ЗАС и защита от вторжений, аудит безопасности ЗАС и управление рисками.

В результате изучения дисциплины, студент должен обладать следующими профессиональными компетенциями (ПК):

ОПК-7: способность определять виды информации, виды угроз безопасности информации и возможные методы реализации угроз на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты;

ПК-1: способность выполнять работы по обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств ЗИ;

ПК-3: способность применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач;

ПК-7: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации.

В результате изучения дисциплины бакалавр должен:

Знать:

- принципы построения информационных систем;
- принципы организации информационных систем в соответствии с требованиями по защите информации;
- основные нормативные правовые акты в области информационной безопасности и защиты, а также нормативные методические документы Федеральной службы безопасности Российской федерации.

Уметь:

- осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
- анализировать и оценивать угрозы информационной безопасности объекта;
- применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.

Владеть:

- методами и средствами выявления угроз безопасности автоматизированным системам;
- навыками организации и обеспечения режима секретности;
- методами технической защиты информации.