Приложение 3

Аннотация к рабочей программе дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем»

по направлению 10.03.01 «Информационная безопасность»
(профиль «Безопасность автоматизированных систем»).

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 ч).
Предполагаемые семестры: 8
Форма контроля: экзамен

Целями освоения дисциплины « Комплексное обеспечение информационной безопасности автоматизированных систем» состоят:
- в изучении способов разработки и реализации мер по защите информационных ресурсов автоматизированных систем (АС);
- в решении задач, требующих классификации и структуризации мер обеспечения безопасности АС от степени конфиденциальности.

Задачами курса являются: анализ и оценка угрозы информационной безопасности объекта; применение отечественных и зарубежных стандартов в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем. Изучение принципов построения и организации информационных систем в соответствии с требованиями по защите информации; основных нормативных правовых актов в области информационной безопасности и защиты, а также нормативных методических документов ФСБ РФ; мер противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

Учебная дисциплина «Комплексное обеспечение информационной безопасности автоматизированных систем» является самостоятельным элементом в системе подготовки специалиста, относится к циклу Б1.В.ДВ. 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 «Комплексное обеспечение информационной безопасности автоматизированных систем» определяются теоретические основы и практические навыки, при освоении которых студент способен приступить к изучению следующих дисциплин в соответствии с учебным планом:
- интегрированные информационные системы в управлении.

Краткое содержание дисциплины:
Постановка проблемы комплексного обеспечения информационной безопасности АС. Состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ). Интеграция средств информационной безопасности в технологическую среду. Стадии и этапы создания КСИБ. Типовая структура программно-технического комплекса. Методы и методики оценки качества КСИБ.
Аттестация и сертификация систем и средств защиты информации.

В результате изучения дисциплины специалист должен обладать следующими профессиональными компетенциями:

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 установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации;
ПК-5: способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты;
ПК-6: способность принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия требованиям защиты информации;
ПК-7: способность принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;
ПК-15: способность принимать участие в формировании комплекса мер по обеспечению информационной безопасности, разрабатывать предложения по совершенствованию системы управления информационной безопасностью;
ПК-16: Способность организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий 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 РФ.
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.