Аннотация

к рабочей программе дисциплины

«Информационная безопасность открытых систем»

по направлению 10.03.01 «Информационная безопасность»

(профиль «Безопасность автоматизированных систем»)

Общая трудоемкость дисциплины составляет 3 зачетных единиц.(108 часов)

Форма контроля: зачет 7 семестр.

Предполагаемые семестры: 7

Цели освоения дисциплины « Информационная безопасность открытых систем» состоят:

- в изучении способов разработки и реализации мер по защите информационных ресурсов автоматизированных открытых систем (АОС);
- в решении задач, требующих классификации и структуризации мер обеспечения безопасности АОС от степени конфиденциальности.

Учебная дисциплина

Дисциплина является самостоятельным элементом в системе подготовки специалиста, относится к циклу Б1.В.ДВ4.1. Для освоения дисциплины необходимы знания, полученные при изучении следующих дисциплин:

- основы информационной безопасности;
- принципы построения, проектирования и эксплуатации автоматизированных информационных систем;
- теоретические основы компьютерной безопасности.

В дисциплине «Информационная безопасность открытых 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:

Эталонные модели среды и взаимосвязи открытых систем.
Обзор зарубежного законодательства и Российского законодательств в области информационной безопасности.
Политика информационной безопасности АОС.
Управленческие и организационные меры по обеспечению ИБ.
Анализ и управление рисками при реализации ИБ.
Архитектурная и технологическая безопасность.
Соотношение эффективности и рентабельности систем ИБ
Методология анализа защищенности информационной системы.
Типовая структура программно-технического комплекса защиты АОС.

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

ПК-6: способность принимать участие в организации и сопровождении аттестации объекта информатизации на предмет соответствия требованиям защиты информации;

ПК-8: способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.

В результате изучения дисциплины бакалавр должен:

Знать:

- 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:

- анализировать и оценивать угрозы информационной безопасности объекта;
- применять отечественные и зарубежные стандарты в области ИБ для проектирования, разработки и оценки защищенности открытых автоматизированных систем.

Владеть:

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