АННОТАЦИЯ
к рабочей программе дисциплины
«Информационная безопасность и защита информации»

Направление подготовки 27.03.04 Управление в технических системах
Профиль Управление и информатика в технических системах
Квалификация выпускника бакалавр
Нормативный период обучения 4 года
Форма обучения очная
Год начала подготовки 2023

Цель изучения дисциплины:

ознакомление студентов с основами комплексного подхода к обеспечению информационной безопасности (ИБ) автоматизированных систем (АС), проблемами защиты информации и подходами к их решению, а так же способам и приёмам защиты информации криптографическими средствами.

Задачи изучения дисциплины:

приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в управлении информационной безопасностью, оценки рисков информационных ресурсов предприятия и аудита информационной безопасности, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности (ИБ) автоматизированных систем.

Перечень формируемых компетенций:

ПК-2 - Способен осуществлять разработку методического обеспечения автоматизированных систем управления производством, планирование предварительных испытаний автоматизированных систем.

Знать основные методы управления информационной безопасностью.

Уметь пользоваться моделями безопасности КС при управлении доступом и информационными потоками.

Владеть навыками анализа информационной инфраструктуры автоматизированной системы и ее безопасности

ПК-5 - Способен к разработке отдельных разделов проекта на различных стадиях проектирования автоматизированных систем управления технологическими процессами

Знать требования информационной безопасности при эксплуатации автоматизированной системы

Уметь оценивать информационные риски в автоматизированных системах и разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы;

Владеть методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем.

Общая трудоемкость дисциплины: 3 з.е.

Форма итогового контроля по дисциплине: Зачет