Аннотация к рабочей программе дисциплины «Защита информации на объектах критической информационной инфраструктуры»

Направление подготовки: 09.04.01 Информатика и вычислительная техника

Направленность (профиль): Информационные технологии в топливно-энергетическом комплексе

Квалификация выпускника: магистр

Цель освоения дисциплины: приобретение знаний обеспечения информационной безопасности на объектах критической информационной инфраструктуры (ОКИИ) и навыков, которые можно применить в начале работы в качестве специалиста по обеспечения безопасности на критических объектах электроэнергетики.

Объем дисциплины: 3 з.е., 108 часов

Семестр: 4

Краткое содержание основных разделов дисциплины:

№ п/п раздела	Основные разделы дисциплины	Краткое содержание разделов дисциплины
1	Основные понятия в области защиты критической информационной инфраструктуры (КИИ)	Актуальность обеспечения информационной безопасности на объектах КИИ. Особенности промышленной IT-инфраструктуры Влияние инцидентов информационной безопасности на работоспособность и отказоустойчивость киберфизических систем. Субъекты и объекты КИИ.
2	Нормативная правовая база в области защиты КИИ	Государственная политика в области обеспечения безопасности информации на объектах критической информационной инфраструктуры.
3	Категорирование объектов КИИ	Классификация объектов КИИ. Стадии категорирования объектов КИИ. Разработка модели угроз безопасности информации объекта ТЭК Анализ рисков информационной безопасности объекта ТЭК
4	Организационные меры обеспечения безопасности информации на значимых объектах КИИ	Описание типового объекта защиты. Основные векторы атак. Требования к организационным мерам обеспечения ИБ на значимых объектах КИИ
5	Технические меры обеспечения безопасности информации на значимых объектах КИИ	Требования к системе обеспечения информационной безопасности значимых объектов КИИ. Основные подсистемы и комплексы технических средств защиты информации. Разработка топологии промышленной сети с комплексом межсетевого экранирования в Cisco Packet Tracer. Применение сетевых сканеров безопасности для оценки защищенности объектов КИИ

Форма промежуточной аттестации: зачет