Аннотация к рабочей программе дисциплины

Автор: Антонова О.В., старший преподаватель

Наименование дисциплины: Б1.В.03 Безопасность вычислительных сетей

Цели освоения дисциплины:

Подготовка к разработке системы управления информационной безопасностью автоматизированных систем, администрирование подсистем информационной безопасности автоматизированных систем

1. Требования к результатам освоения дисциплины:

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине (модулю)**
ПК-2 Способен администрировать средства защиты информации в компьютерных системах и сетях	ПК-2.1 Осуществляет выбор и настройку средств защиты информации в компьютерных системах и сетях	*Знать:* организацию взаимодействия в вычислительных сетях *Уметь:* осуществлять настройку основных параметров безопасности сетевого взаимодействия. *Владеть:* Навыками конфигурирования сетевого и телекоммуникационного оборудования для обеспечения безопасности сетевого взаимодействия.

ПК-3 Способен анализировать и противодействовать угрозам информации операционных систем, систем управления базами данных, вычислительных сетей	ПК-3.1 Выявляет потенциальные угрозы	*Знать:* перспективные направления обеспечения информационной безопасности в вычислительных сетях; актуальные подходы к реализации безопасного информационного обмена и надежного функционирования компьютерных сетей; типичные уязвимости и способы реализации основных сетевых атак *Уметь:* применять стандартные средства и технологии обеспечения защиты сетевой топологии и безопасной работы вычислительных сетей; организовывать защищенный информационный обмен в компьютерных вычислительных сетях; реализовывать комплекс защитных мероприятий для обеспечения безопасности функционирования вычислительных сетей; строить политики сетевой безопасности и фильтрации сетевого трафика; *Владеть:* навыками анализа сетевых информационных систем с позиции обеспечения информационной безопасности; методикой планирования и обеспечения защитных мероприятий на компьютерных вычислительных сетях; навыками применения защищенных протоколов сетевого обмена, средств контроля доступа и фильтрации трафика в вычислительных сетях и сетевых информационных системах.
ПК-3 Способен анализировать и противодействовать угрозам информации операционных систем, систем управления базами данных, вычислительных сетей	ПК-3.2 Разрабатывает меры противодействия потенциальным угрозам	*Знать:* основные сервисы безопасности в сетях; современные протоколы и принципы построения безопасных сетей передачи данных. *Уметь:* применять современные методы защиты при решении проблем информационной безопасности в сетях. *Владеть:* знаниями о современных методах защиты при решении проблем информационной безопасности в сетях.

2. Содержание дисциплины:

Тема 1. Основы вычислительных сетей. Сетевая архитектура.

Тема 2. Технологии обеспечения безопасности в сетях Типовые угрозы сетевой безопасности.

Тема 3. Построение защищенных сетей на базе сетевых операционных систем: Сетевые операционные системы (ОС) NetWare, Windows, UNIX.

Тема 4. Глобальная сеть Интернет.

Тема 5. Безопасности сети Интернет.

Тема 6. Комплексная защита подключения к Интернет.

3. Общая трудоёмкость дисциплины: 3 ЗЕ.