МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ (МОДУЛЯ)
«Модели и методы обеспечения безопасности распределенных систем»
Научная специальность: 2.3.6. Методы и системы защиты информации,
информационная безопасность
форма обучения (очная)

Объем дисциплины (модуля): 3 (з.е.)

Форма промежуточной аттестации: дифференцированный зачет.

Цели и задачи освоения дисциплины:

Целью изучения дисциплины «Модели и методы обеспечения безопасности распределенных систем» является теоретическая и практическая подготовка аспирантов к деятельности, связанной с защитой данных в информационной системе; обучение базовым принципам информационной безопасности, моделям и методам защиты информации распределительных систем.

Задачи дисциплины:

изучение основных методов и принципов обеспечения конфиденциальности, целостности и доступности информации распределительных систем;

изучение типовых угроз безопасности информации при ее обработке в информационных системах;

изучение основных принципов обеспечения информационной безопасности;

изучение основ построения модели угроз и политики безопасности;

изучение основных моделей доступа.

Планируемые результаты освоения:

В результате освоения дисциплины у обучающегося формируются компетенции:

ПК-2 - способность к разработке и реализации принципов и решений (технических, математических, организационных и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.

ПК-9 - способность к созданию новых и совершенствованию существующих моделей и методов оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты вне зависимости от области их функционирования.

ПК-14 - готовность к проведению комплексных исследований научных и технических проблем с применением математического моделирования, вычислительного эксперимента и программных средств.

Краткое содержание дисциплины:

Тема 1. Классификация угроз информационной безопасности;

Тема 2. Нормативно-правовой подход к обеспечению информационной безопасности;

Тема 3. Практический (экспериментальный) подход к обеспечению информационной безопасности;

Тема 4. Определение и разработка политики безопасности;

Тема 5. Аудит информационной безопасности.