Аннотация рабочей программы дисциплины
«Информационная безопасность»

Цель дисциплины − формирование у обучаемых потребности в постоянном развитии своих знаний и способностей их эффективного использования в области теоретических основ и технологий информационной безопасности (ИБ) и защиты информации (ЗИ);

— освоения умений и навыков практического обеспечения должной информационной безопасности (ИБ) при создании, модификации и сопровождении автоматизированных информационных систем (АИС), правильном администрировании их баз данных (БД) в строгом соответствии со стратегией развития искусственного интеллекта в Российской федерации (РФ) на период до 2030 года.

Такая целевая установка способствует быстрому развитию искусственного интеллекта (ИИ) - комплексу технологических решений, позволяющих имитировать когнитивные (познавательные) функции человека (включая самообучение и поиск управленческих решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека. Такой комплекс включает в себя информационно-коммуникационную инфраструктуру (ИКС), программное обеспечение (ПО), в котором используется методы машинного обучения, процессы и сервисы по обработке данных и быстрому поиску правильных управленческих решений. При этом ИИ обеспечивает эффективное использование программных средств и технологий систем ИБ и ЗИ в вычислительных системах и сетях (ВСС).

Задачи дисциплины

- Анализ возможностей по управлению вычислительными ресурсами, взаимодействующими с БД;
- Управления вычислительными ресурсами, взаимодействующими с БД.

Названия тем, основных вопросов в виде дидактических единиц:

Национальная стратегия развития ИИ в РФ и ее связь с ИБ 1 Цели и задачи стратегии, ее основные понятия. 2 Принципы и технологии стратегии, их использование в совершенствовании ИБ в РФ. 3 Механизм совершенствования ИБ с учетом реализации стратегии развития ИИ.
Объект и предмет ИБ. 1 Угрозы и концепция ИБ. 2 Цели и задачи дисциплины. 3 Направления обеспечения ИБ
Системы защиты информации (СЗИ) от случайных угроз, традиционного шпионажа и диверсий. 1. Классификация угроз. 2. Случайные и преднамеренные угрозы.
СЗИ от побочных электромагнитных излучений и наводок (ПЭМИН). 1.Методы защиты от ПЭМИН. 2. Средства выявления и защиты от ПЭМИН. 3. Активные методы защиты от ПЭМИН.
Защита информации (ЗИ) от несанкционированного доступа (НСД). 1. Общие требования к защищенности от НСД 2. Защита от программных и аппаратных закладок. 3. Защита от несанкционированных изменений структур
Компьютерные вирусы (КВ) и механизмы борьбы с ними. 1. Классификация КВ. 2. Принципы и методы защиты от КВ. 3. Профилактика заражений КВ в АИС.

Принципы применения криптографической защиты информации 1. Классификация методов криптографического преобразования информации. 2. Стандарты шифрования. 3. Перспективы использования шифрования в АИС.
Стенографическая защита информации. 1. Основные понятия стенографии. 2. Основные угрозы стенографии и типы нарушителей. 3. Компьютерная и цифровая стенография.
ЗИ в распределенных компьютерных системах (РКС). 1. Архитектура РКС. 2. Обеспечение ИБ в пользовательской подсистеме и специализированных РКС. 3. ЗИ на уровне подсистем управления РВС.
Особенности ЗИ в распределенных компьютерных систем (РКС). 1. Концепция создания защищенных РКС. 2. Методология проектирования защищенных РКС 3. Этапы создания РКС
Теория компьютерных систем защиты информации (КСЗИ). 1. Математическая постановка задачи разработки КСЗИ 2. Моделирование и реализация КСЗИ. 2. Эксплуатация КСЗМ.

Объем дисциплины 4 з.е.

Форма промежуточного контроля – *экзамен.*