Аннотация рабочей программы дисциплины
по направлению 01.03.02 Прикладная математика и информатика
профиль: Математическое моделирование

Основы информационной безопасности

Цели и задачи освоения дисциплины

Цель дисциплины — овладеть методами и технологиями защиты информации на автоматизированных рабочих местах и в локальных вычислительных сетях на основе:

- требований существующих нормативно-правовых актов и стандартов к организации защиты информации;
- анализа возможных угроз информационным активам и оценкой уязвимостей информационных систем;
- применения инженерно-технических, программно-аппаратных и организационных механизмов защиты информации.

В задачи дисциплины входит:

- ознакомить студентов с терминологией в сфере информационной безопасности и основными положениями существующих концепций и нормативно-правовых актов по организации защиты информации;
- овладеть методологией анализа возможных угроз информационным активам, оценкой уязвимостей информационных систем оценкой ценности информационных активов организации;
- ознакомиться с механизмами эффективной защиты информационных активов организации.

Место дисциплины в структуре ОПОП ВО

Дисциплина «Основы информационной безопасности» относится к обязательной части образовательной программы, по направлению 09.03.03 Прикладная информатика.

Дисциплина изучается в 6 семестре очной формы обучения, форма промежуточной аттестации –зачет с оценкой.

Перечень дисциплин с указанием разделов (тем), предшествующих дисциплине «Основы информационной безопасности»:

Семестр	Дисциплина	Разделы
1	Введение в программирование	Типы алгоритмов. Операторы, отвечающие за логику программы. Алгоритмы с использованием условных и циклических конструкций. Алгоритмы работы с массивами. Алгоритмы обработки двумерных массивов
		Классы, конструкторы, методы, способы передачи параметров в методы. Файловая система. Работа с текстовым файлом.
2	Объектно-ориентированное программирование	Объектный подход к разработке программного обеспечения. Объекты: абстракция, ограничение доступа, модульность, иерархия, типизирование, параллелизм, устойчивость. Идентификация классов и объектов

		Объектный подход, как общий принцип создания программного обеспечения в среде Windows и C#. Класс Application. Организация работы с несколькими формами в приложении. Модальные формы, их особенности, критерии обоснованности выбора при проектировании
5	Операционные системы	Классификация ОС. Структура современной ОС (на примере MS Windows NT, UNIX). Основные компоненты ОС и их взаимодействие. Ядро ОС, службы ОС, оболочка ОС.
		Безопасность и надежность операционных систем. Права пользователей и программ. Система доступа к объектам ОС в современных ОС. Пароли, защищенные протоколы связи. Криптография, симметричные и асимметричные системы шифрования. Отказоустойчивые программно-технические комплексы/ Поддержка вычислительных сетей в ОС. Сетевые протоколы. Многоуровневая модель сети ISO/OSI.

Содержание дисциплины

№	Содержание раздела
Раздел 1	Введение. Основные термины и определения: Термины, определения, основные понятия, природа угроз ИБ, каналы утечки информации, общая и частная модели угроз, модель нарушителя, иерархия требований в области информационной безопасности.
Раздел 2	Обзор законодательных требований в области защиты информации: обзор 149-ФЗ; Персональные данные (152-ФЗ); Коммерческая тайна (98-ФЗ); Критическая информационная инфраструктура (187-ФЗ), Государственная тайна; Иные конфиденциальные требования.
Раздел 3	Защита (безопасность) информационных систем: Основные задачи, меры и методы противодействия угрозам ИБ (классификация, определение), основные принципы построения систем защиты. Модели безопасности: состав моделей, описание угроз, обоснование.
Раздел 4	Организационные методы защиты: Правовой статус. Иерархия управления. Определение ответственности. Локально-нормативные акты. Обязанности и ответственности. Инструктажи. Прочая регламентация деятельности. Политика информационной безопасности. Ответственность за нарушение в области информационной безопасности (Уголовный кодекс РФ. Кодекс об административных правонарушениях РФ. Гражданский кодекс РФ — обзор статей).
Раздел 5	Технические методы защиты: Криптография и стеганография. Обзор методов шифрования и встраивания. Методы криптоанализа. Методы стеганоанализа. Пароли. Парольные политики. Разграничение доступа в операционных средах UNIX и Windows. Требования к стойкости, защите и методы атак. Вирусы. Кибербезопасность и защита от взлома. Анализ защищенности с использованием автоматизированных инструментов. IDS-системы. Системы анализа уязвимостей (локальные и сетевые). Антивирусные средства.

Раздел 6	Мероприятия по защите объектов информатизации и контроль их эффективности (обзор): Разграничение доступа к объектам информатизации, защищаемым помещениям. Формирование списков лиц, допущенных к ограниченным материалам. Контроль эффективности. Аудит предприятия. Выводы. Корректирующие мероприятия. Оценка эффективности.
Раздел 7	Применение стандартов в области информационной безопасности (обзор): Общие критерии безопасности информационных технологий. Серия стандартов ГОСТ Р ИСО/МЭК 15408 (обзор). Системы менеджмента информационной безопасности (СМИБ). Серия стандартов ГОСТ Р ИСО/МЭК 27000 (обзор).