ИНДИВИДУАЛЬНЫЕ ПРАКТИЧЕСКИЕ РАБОТЫ, ИХ ХАРАКТЕРИСТИКА

Введение

По результатам работы по каждому заданию студентом должен быть представлен и защищен отчет. Содержание отчета включает:

1) Титульный лист
2) Введение, содержащее постановку задачи и пошаговое описание использованного алгоритма.
3) Блок – схему алгоритма.
4) Распечатку скриншотов результатов ввода данных и исполнения программы.
5) Распечатку программного кода.
6) Вывод.

ИПР. Криптографические методы защиты информации.

Цель:

Реализовать Программное средство идентификации и аутентификации пользователей с использованием протокола Kerberos.

Общая постановка задачи:

1) Изучить теоретические сведения.
2) Создать приложение, реализующее протокол распределения ключей Kerberos, включая процедуру, реализующую Алгоритм DES.

В интерфейсе приложения должны быть наглядно представлены:

- ✓ Исходные данные протокола (модули, ключи, секретные данные и т.п.);
- ✓ Данные, передаваемые по сети каждой из сторон;
- ✓ Проверки, выполняемые каждым из участников.

Процесс взаимодействия между сторонами протокола может быть реализован при помощи буферных переменных. Также необходимо выделить каждый из этапов протоколов для того, чтобы его можно было отделить от остальных.

Результат:

Программа, осуществляющая идентификацию и аутентификацию модельных пользователей с использованием протокола Kerberos на базе процедуры Алгоритма DES.