Лабораторная работа№6

ТЕМА:«ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ»

Выполнила:
Айчаракова Фарида

Содержание

1. Средства защита информации от несанкционированного доступа
2. Защита использованием паролей
3. Защита от вредоносных программ

3.1 Вредоносные и антивирусные программы

3.2 Компьютерные вирусы и защита от них

4 Биометрические системы защиты

Средства защита информации от несанкционированного доступа

Несанкционированный доступ (НСД) к информации – доступ, нарушающий установленные правила разграничения доступа. Субъект, осуществляющий НСД, является нарушителем правил разграничения доступа. НСД является наиболее распространенным видом нарушений безопасности информации

Для защиты от несанкционированного доступа к программам и данным используются – пароли

Компьютер разрешает доступ к своим ресурсам только тем пользователям, которые зарегистрированы и ввели правильный пароль. Каждому конкретному пользователю может быть разрешен доступ только к определенным информационным ресурсам. При этом может производиться регистрация всех попыток несанкционированного доступа.

Защита с использованием пароля используется при загрузке операционной системы

Вход по паролю может быть установлен в программе BIOS Setup, компьютер не начнет загрузку операционной системы, если не введен правильный пароль. Преодолеть такую защиту нелегко.

От несанкционированного доступа может быть защищены

- каждый диск,
- каждая папка,
-каждый файл локального компьютера.

Для них могут быть установлены определенные права доступа полный доступ,

- возможность внесения изменений,
- только чтение, запись и др.

Права могут быть различными для различных поль

Вредоносная программа -злонамеренная программа, то есть программа, созданная со злым умыслом и/или злыми намерениями. Защита от вредоносных программ.

Вредоносная программа

- Вирусы, черви, троянские и хакерские программ
- Шпионское, рекламное программное обеспечение
- Потенциально опасное программное обеспечение

Антивирусные программы

Современные антивирусные программы обеспечивают комплексную защиту программ и данных на компьютере от всех типов вредоносных программ и методов их проникновения на компьютер:

-Интернет,

-локальная сеть,

-электронная почта,

-съемные носители информации.

Для защиты от вредоносных программ каждого типа в антивирусе предусмотрены отдельные компоненты.

Принцип работы антивирусных программ основан на проверке файлов, загрузочных секторов дисков и оперативной памяти и поиске в них известных и новых вредоносных программ.

Антивирусные программы

Для поиска известных вредоносных программ используются сигнатуры. Сигнатура- это некоторая постоянная последовательность программного кода, специфичная для конкретной вредоносной программы. Если антивирусная программа обнаружит такую последовательность в каком-либо файле, то файл считается зараженным вирусом и подлежит лечению или удалению.

Для поиска новых вирусов используются алгоритмы эвристического сканирования, т. е. анализа последовательности команд в проверяемом объекте. Если «подозрительная» последовательность команд обнаруживается, то антивирусная программа выдает сообщение о возможном заражении объекта.

Биометрические системы защиты

В настоящее время для защиты от несанкционированного доступа к информации все более часто используются биометрические системы идентификации.

Используемые в этих системах характеристики являются неотъемлемыми качествами личности человека и поэтому не могут быть утерянными и подделанными.

К биометрическим системам защиты информации относятся системы идентификации:

- по отпечаткам пальцев;
- по характеристикам речи;
- по радужной оболочке глаза;
- по изображению лица;
- по геометрии ладони руки.

Идентификация по отпечаткам пальцев

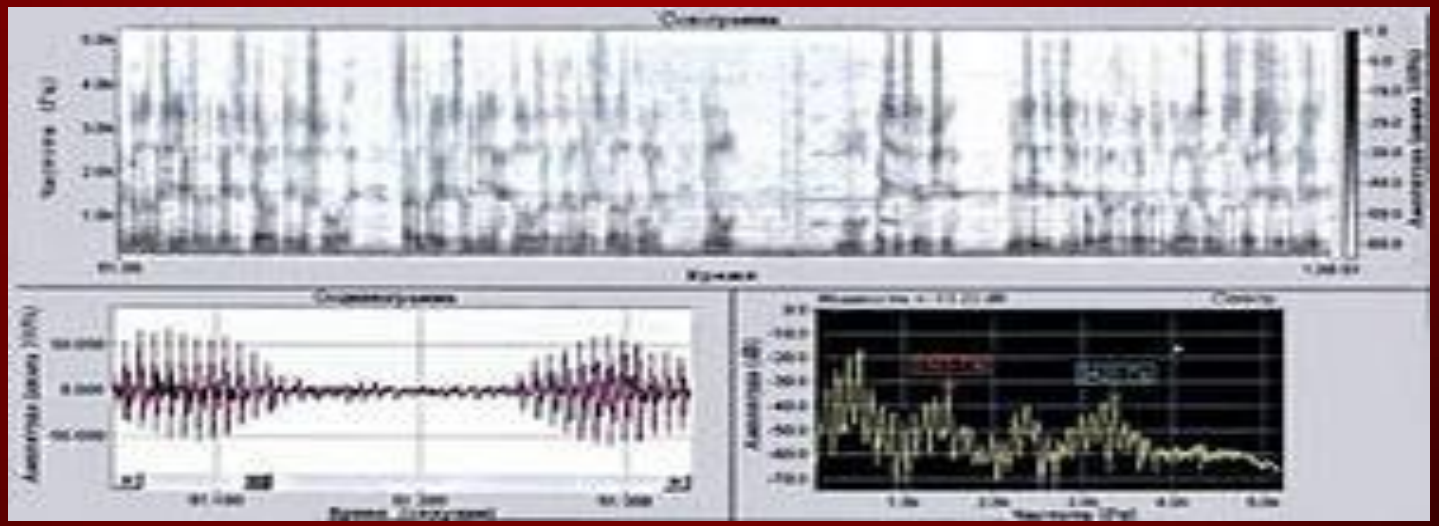
Оптические сканеры считывания отпечатков пальцев устанавливаются на ноутбуки, мыши, клавиатуры, флэш-диски, а также применяются в виде отдельных внешних устройств и терминалов (например, в аэропортах и банках).

Если узор отпечатка пальца не совпадает с узором допущенного к информации пользователя, то доступ к информации невозможен.

Идентификация по характеристикам речи

Идентификация человека по голосу один из традиционных способов распознавания, интерес к этому методу связан и с прогнозами внедрения голосовых интерфейсов в операционные системы.

Голосовая идентификация бесконтактна и существуют системы ограничения доступа к информации на основании частотного анализа речи.



нтификация по радужной оболочке глаза

Для идентификации по радужной оболочке глаза применяются специальные сканеры, подключенные к компьютеру. Радужная оболочка глаза является уникальной для каждого человека биометрической характеристикой.

Изображение глаза выделяется из изображения лица и на него накладывается специальная маска штрих-кодов. Результатом является матрица, индивидуальная для каждого человека.

Идентификация по ладони руки

В биометрике в целях идентификации используется простая геометрия руки размеры и форма, а также некоторые информационные знаки на тыльной стороне руки (образы на сгибах между фалангами пальцев, узоры расположения кровеносных сосудов).

Сканеры идентификации по ладони руки установлены в некоторых аэропортах, банках и на атомных электростанциях.