Лабораторная работа №10

Тема «Реализация системы защиты программными средствами»

ВЫПОЛНИЛ

Ганевич Андрей

Группа 25-ПО

Задание: исследовать методы реализации систем защиты программными средствами.

Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств – универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки – ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

Среди них можно выделить и подробнее рассмотреть следующие:

1. средства архивации данных;
2. антивирусные программы;
3. криптографические средства;
4. средства идентификации и аутентификации пользователей;
5. средства управления доступом;
6. протоколирование и аудит.

Как примеры комбинаций вышеперечисленных мер можно привести:

1. защиту баз данных;
2. защиту информации при работе в компьютерных сетях.

Средства архивации информации

Иногда резервные копии информации приходится выполнять при общей ограниченности ресурсов размещения данных, например, владельцам персональных компьютеров. В этих случаях используют программную архивацию. Архивация — это слияние нескольких файлов и даже каталогов в единый файл — архив, одновременно с сокращением общего объема исходных файлов путем устранения избыточности, но без потерь информации, т. е. с возможностью точного восстановления исходных файлов. Действие большинства средств архивации основано на использовании алгоритмов сжатия, предложенных в 80-х гг. Абрахамом Лемпелем и Якобом Зивом. Наиболее известны и популярны следующие архивные форматы:

1. ZIP, ARJ для операционных систем DOS и Windows;
2. TAR для операционной системы Unix;
3. межплатформный формат JAR (Java ARchive);
4. RAR (все время растет популярность этого нового формата, так как разработаны программы позволяющие использовать его в операционных системах DOS, Windows и Unix).

Пользователю следует лишь выбрать для себя подходящую программу, обеспечивающую работу с выбранным форматом, путем оценки ее характеристик – быстродействия, степени сжатия, совместимости с большим количеством форматов, удобности интерфейса, выбора операционной системы и т.д. Список таких программ очень велик – PKZIP, PKUNZIP, ARJ, RAR, WinZip, WinArj, ZipMagic, WinRar и много других. Большинство из этих программ не надо специально покупать, так как они предлагаются как программы условно-бесплатные (Shareware) или свободного распространения (Freeware). Также очень важно установить постоянный график проведения таких работ по архивации данных или выполнять их после большого обновления данных.

Основные направления защиты информации. Основные направления использования программной защиты информации:

1. защита информации от НСД;
2. защита программ от копирования;
3. защита информации от разрушения;
4. защита информации от вирусов;
5. защита программ от вирусов;
6. программная защита каналов связи;



Рисунок 1 – Средства программной защиты

Защита информации от НСД. Для защиты от чужого вторжения обязательно предусматриваются определенные меры безопасности. Особые функции, которые должны осуществляться программными средствами, это:

1. идентификация объектов и субъектов;
2. разграничение (иногда полная изоляция) доступа к вычислительной технике;
3. контроль и регистрация действий с информацией и программами.

В процедурах идентификации используются различные методы:

1. простые, сложные и одноразовые пароли;
2. обмен вопросами и ответами с администратором;
3. средства анализа индивидуальных характеристик;
4. ключи, магнитные карты, значки и т.д.;
5. специальные идентификаторы или контрольные суммы для аппаратуры.

После идентификации защита осуществляется на 3 уровнях:

1. аппаратуры;
2. программного обеспечения;
3. данных.

Защита на уровне аппаратуры и программного обеспечения предусматривает управление доступом к вычислительным ресурсам. Защита на уровне данных направлена на защиту информации при обращении к ней в процессе работы и на защиту информации при ее передаче по каналам связи.

Средства регистрации, как и средства контроля доступа, относятся к эффективным методам защиты от НСД. Однако, если средства контроля доступа предназначены для предотвращения таких действий, то задача регистрации – обнаружить уже совершенные действия.