ЛАБОРАТОРНАЯ РАБОТА №1

ЗАЩИТА ОТ РАЗРУШАЮЩИХ ПРОГРАММНЫХ ВОЗДЕЙСТВИЙ, ЗАЩИТА ПРОГРАММ ОТ ИЗМЕНЕНИЯ И КОНТРОЛЬ ЦЕЛОСТНОСТИ

1. ЦЕЛЬ РАБОТЫ

Познакомиться с общими принципами защиты программного обеспечения и способами организации контроля целостности исполняемых модулей и важных программных данных.

2. КРАТКИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

В основе каждого программного продукта лежит интеллектуальная собственность его разработчиков. Ведь на создание программы ушло много часов работы программистов, тестировщиков и службы маркетинга. Хочется, чтобы при коммерческом релизе уникальный продукт не был скопирован и модифицирован конкурентами, а для этого программы необходимо защищать от изменения.

Основным методом борьбы с модификацией является контроль целостности. Реализация этого может быть достигнута методами проверки контрольной суммы и цифровой подписью.

Цифровая подпись

Электронная цифровая подпись (**ЭЦП**) — реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования **ЭЦП** и проверить принадлежность подписи владельцу сертификата ключа ЭЦП. Значение реквизита получается в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП.

Подпись лучше всего использовать для контроля целостности статических данных. Она будет записана в конец файла и при необходимости проверена.

Контрольная сумма

Контрольная сумма — некоторое значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении. Так же контрольные суммы могут использоваться для быстрого сравнения двух наборов данных на неэквивалентность: с большой вероятностью различные наборы данных будут иметь неравные контрольные суммы. Это может быть использовано, например, для детектирования компьютерных вирусов.

Для подсчета контрольной суммы можно использовать алгоритм MD5 и соответствующее программное обеспечение, например MD5-калькуляторы [7].

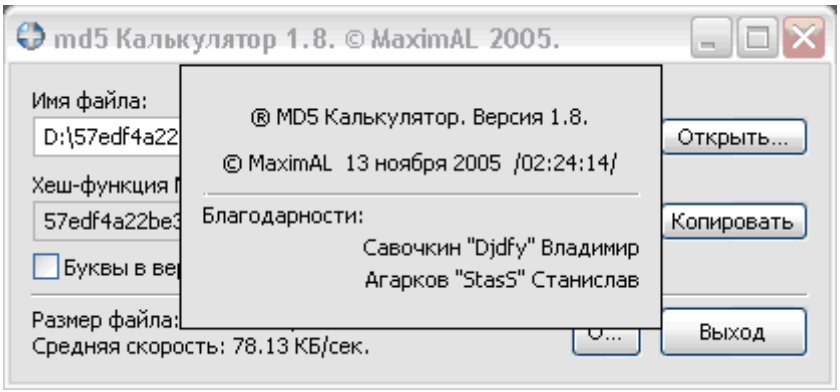

Рис. 1

Если речь идет о приложении или библиотеке, то можно реализовать функцию проверки на соответствие вычисленной ранее контрольной суммы только что рассчитанной. В случае совпадения значений программа или библиотека будет продолжать выполнение, иначе – завершать работу. Целесообразно выполнять такую функцию перед каждым запуском приложения и при каждом входе в библиотеку dll.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить вариант задания у преподавателя.
2. Разработать программу.
3. Продемонстрировать выполнение программы преподавателю, сравнить полученный результат с ожидаемым.
4. Оформить и защитить отчет.

4. ТРЕБОВАНИЯ К ОФОРМЛЕНИЮ ОТЧЕТА

Отчет по лабораторной работе должен содержать следующие разделы:

- задание по лабораторной работе;
- описание алгоритма работы программы;
- листинг программы;
- выводы по проделанной работе.

5. ВАРИАНТЫ ЗАДАНИЙ

1. Контроль целостности исполняемого модуля Win32.
2. Контроль целостности используемых Win32 библиотек.
3. Контроль целостности программных данных (данные неизменны).
4. Контроль целостности определенных директорий.
5. Контроль целостности файла содержащего неизменные данные в каталоге /usr ОС Astra Linux Common Edititon.
6. Контроль целостности созданного каталога в каталоге /usr в ОС Astra Linux Common Edititon.