# *Практическая работа № 17*

**Организация защиты при помощи компакт-дисков и электронных ключей**

Цель работы: изучение опыта организации защиты информации с помощью компакт-дисков и электронных ключей

Теоретическое обоснование

  Защита при помощи компакт-дисков

Программа может требовать оригинальный компакт-диск. В частности, такой способ применяется в играх. Стойкость таких защит невелика, ввиду широкого набора инструментов снятия образов компакт-дисков.

Как правило, этот способ защиты применяется для защиты программ, записанных на этом же компакт-диске, являющимся одновременно ключевым.

Для защиты от копирования используется:

* запись информации в неиспользуемых секторах;
* проверка расположения и содержимого «сбойных» секторов;
* проверка скорости чтения отдельных секторов.

Первые два метода практически бесполезны из-за возможности снятия полного образа с диска с использованием соответствующего прикладного ПО. Третий метод считается более надежным (используется, в частности, в защите StarForce). Но существуют программы, которые могут эмулировать диски с учётом геометрии расположения данных, тем самым обходя и эту защиту. В StarForce, в числе прочих проверок, также выполняется проверка возможности записи на вставленный диск. Если она возможна, то диск считается не лицензионным. Однако, если образ будет записан на диск CD-R, то указанная проверка пройдет. Существует возможность скрыть тип диска, чтобы CD-R или CD-RW был виден как обычный CD-ROM. Однако, в драйвер защиты может быть встроена проверка на наличие эмуляции.

В настоящее время наибольшую известность в мире имеют системы защиты от копирования SecuROM, StarForce, SafeDisc, CD-RX и Tages.

Для многих программ указанный метод защиты недоступен ввиду отличного способа распространения (например, shareware-программы).

Защита при помощи электронных ключей

Электронный ключ предотвращает незаконное использование (эксплуатацию) программы. Часто говорят, что ключ защищает от копирования, но это не совсем верно. Защищенную программу можно скопировать, только копия без ключа работать не будет. Т. о. копирование просто не имеет смысла.

Собственно электронный ключ — это устройство размером, как принято говорить, «со спичечный коробок» , которое подсоединяется к одному из портов компьютера. Ключ состоит из платы с микросхемами (вспомогательные элементы, микроконтроллер и память), заключенной в пластиковый корпус. Микроконтроллер содержит так называемую «математику» — набор команд, реализующих некую функцию или функции, которые служат для генерации информационных блоков обмена ключа и защищенной программы. Иначе эти блоки называются «вопросы и ответы». Память электронного ключа содержит информацию о его характеристиках, а также данные пользователя. Ключ имеет два разъема. С помощью одного он подсоединяется к LPT-порту (параллельному порту) компьютера, другой служит для подключения периферийного устройства. При правильной эксплуатации современный электронный ключ обычно не вносит помех в работу принтеров, сканеров и прочей периферии, которая подключена через него к параллельному порту.

Методические указания

Для выполнения практической работы посетите сайты:

* Электронный ключ — средство предохранения софта — <https://www.guardant.ru/press-center/publication/2001-08-01.html>

Задания

1. Повторите теоретический материал
2. Проведите исследование организации локальной программной защиты
3. Выполните исследование методов локальной программной защиты и оформите его в виде таблицы
4. Таблицу занесите в тетрадь

Контрольные вопросы

1. Как организована защита информации при помощи компакт- дисков?
2. Как организована защита информации при помощи электронных ключей?
3. Что такое токен?
4. Какие организации используют данные средства защиты информации?

Форма отчёта

Конспект, проверка письменной работы, ответы на вопросы