***Билет 14***

**TrueCrypt** — компьютерная программа для шифрования на «лету» для 32- и 64-разрядных операционных систем семейств Microsoft Windows NT 5 и новее (GUI-интерфейс), Linux и Mac OS X. Позволяет создавать зашифрованный логический (виртуальный) диск, хранящийся в виде файла. С помощью TrueCrypt также можно полностью зашифровать раздел жёсткого диска или иной носитель информации, например, USB-флеш-накопитель. Все сохранённые данные в томе TrueCrypt полностью шифруются, включая имена файлов и каталогов. Смонтированный том TrueCrypt подобен обычному логическому диску, поэтому с ним можно работать с помощью обычных утилит проверки и дефрагментации файловой системы.

С помощью TrueCrypt можно создавать зашифрованный виртуальный диск:

1. в файле-контейнере, что позволяет легко работать с ним — переносить, копировать (в том числе на внешние устройства как любой другой обычный файл), переименовывать или удалять;
2. в виде зашифрованного раздела диска, что делает работу более производительной и удобной, в версии 5.0 появилась возможность шифровать системный раздел;
3. путём полного шифрования содержимого устройства, такого как флеш-накопитель (дискеты не поддерживаются начиная с версии 7.0).

Для доступа к зашифрованным данным можно применять пароль (ключевую фразу), ключевые файлы (один или несколько) или их комбинации. В качестве ключевых файлов можно использовать любые доступные файлы на локальных, сетевых, съёмных дисках (при этом используются первые 1 048 576 байт) и генерировать свои собственные ключевые файлы.

Одна из примечательных возможностей TrueCrypt — обеспечение двух уровней правдоподобного отрицания наличия зашифрованных данных, необходимого в случае вынужденного открытия пароля пользователем:

1. Создание скрытого тома, что позволяет задать второй пароль (и набор ключевых файлов) к обычному тому для доступа к данным, к которым невозможно получить доступ с основным паролем, при этом скрытый том может иметь любую файловую систему и располагается в неиспользованном пространстве основного тома.
2. Ни один том TrueCrypt не может быть идентифицирован (тома TrueCrypt невозможно отличить от набора случайных данных, то есть файл нельзя связать с TrueCrypt как с программой, его создавшей, ни в какой форме и рамках).