Protection

There are a variety of security measures that can be used to protect hardware (the physical components of a computer system) and software (programs and data) including:

1) Controlling physical access to hardware and software.

2) Backing up data and programs (storing a copy of files on a storage device to keep them safe).

3) Implementing network controls such as:

-using passwords (a secret code used to control access to a network system)

-installing a firewall (a combination of hardware and software used to control the data going into and out of a network. It is used to prevent unauthorised access to the network by hackers).

-encrypting data (protecting data by putting it in a form only authorized users can understand)

-installing a callback system

-using signature verification or biometric security

4) Separating and rotating the computing functions carried out by employees and carrying out periodic audits of the system observing and recording events on the network systematically.

5) Protecting against natural disasters by installing uninterruptible power supplies

6) Protecting against viruses by using antivirus programs (computer programs or sets of programs used to detect, identify and remove viruses from a computer system) and ensuring that all software is free of viruses before it is installed.

An anti-virus program is a program that checks files for virus coding instructions inside another program and can be used for removing any virus coding instructions detected.

Защита

Существует множество мер безопасности(security measures), которые можно использовать для защиты оборудования (физических компонентов компьютерной системы) и программного обеспечения (программ и данных), в том числе:

1) Контроль физического доступа к аппаратному и программному обеспечению (hardware and software).

2) Резервное копирование(backuping) данных и программ (хранение копии файлов на запоминающем устройстве для их безопасности).

3) Внедрение(implementing) сетевых элементов управления, таких как:

-использование паролей (секретный код, используемый для управления доступом к сетевой системе)

- установка брандмауэра(firewalls) (Он используется для предотвращения(prevent) несанкционированного доступа(unauthorised access) к сети со стороны хакеров).

-шифрование(encrypting) данных (защита данных путем помещения их в форму, понятную только авторизованным пользователям)

-установка системы обратного звонка (callback system)

-использование проверки подписи или биометрической защиты

4) Разделение и чередование (Separating and rotating) вычислительных функций, выполняемых (carried) сотрудниками, и проведение периодических проверок системы, систематическое наблюдение и запись событий в сети.

5) Защита от стихийных бедствий (natural disasters) путем установки источников бесперебойного питания (uninterruptible power supplies).

6) Защита от (protecting against) вирусов с помощью антивирусных программ (компьютерных программ или наборов программ, используемых для обнаружения, идентификации и удаления вирусов из компьютерной системы) и обеспечение отсутствия вирусов во всем программном обеспечении до его установки.

Антивирусная программа — это программа, которая проверяет файлы на (for) наличие инструкций по кодированию вирусов внутри другой программы и может использоваться для удаления любых обнаруженных инструкций по кодированию вирусов.