**Устная тема №6 (SOFTWARE BASICS)**

*1. Types of software*

Software determines the tasks a digital device can help you accomplish. The are two main categories: system software and application software. Operating systems are classified as system software. Device drivers, utilities, and programming languages are also system software. Application software categories include music, graphics, mapping, finance, and entertainment. Application software is designed to help people accomplish real-world tasks, whereas system software is designed for computer-centric tasks. Let’s take a look at some of the applications you might have on your digital devices.

* Music software offers many ways to work with music, sound effects from your computer. The most popular music software capabilities include downloading, playing and recording music files, creating playlists, transferring music to handheld devices.
* A mapping application displays satellite(спутник), aerial(воздушный), or street maps used to locate places and get directions between two addresses. Google Maps is one of the most extensive(обширное) mapping applications.
* Location-based software is able to access your current location and use it to show you the closest shops, restaurants, ATMs, and theaters.
* A device driver is software that helps a peripheral device establish communication with a computer. This type of system software is used by printers, monitors, sound cards, network cards, storage devices, modems, mice, and scanners.
* Database software helps you enter, find, organize, update, and report information stored in a database.

*2. Security threats*

Threat can be anything that can take advantage of a vulnerability (уязвимость) to breach(нарушить) security and negatively alter(изменение), erase(стирание), harm object or objects of interest.

Software attacks means attack by Viruses, Worms, Trojan Horses, bots, and spyware. Many users believe that malware, virus, worms, bots are all same things. But they are not same, only similarity is that they all are malicious software that behave differently.

Theft of intellectual property means violation of intellectual property rights like copyrights, patents.

Identity theft means to act someone else to obtain person’s personal information or to access vital information they have.

*3. Software security*

Security software is designed to protect computers from various forms of destructive software and unauthorized intrusions. The terms malicious software and malware refer to any computer program designed to gain unauthorized access to data, or disrupt normal processing operations.

A computer virus is a set of program instructions that attaches itself to a file, reproduces itself, and spreads to other files.

A security suite integrates several security modules to protect against the most common types of malware, unauthorized access, and spam.

Antivirus software is a type of utility software that looks for and eradicates viruses, trojan horses, worms, and bots. Antivirus software is available for all types of computers and data storage devices. A virus signature is a section of program code, that can be used to identify a known malicious program.

*4. Software piracy*

It seems that illegal software is available anywhere, to anyone, at any time. The following are some of the methods.

The most common type of piracy, softlifting, means sharing a program with someone who is not authorized by the license agreement to use it.

Hard disk loading involves loading an unauthorized copy of software onto a computer being sold to the end user.

Renting involves someone renting out a copy of software for temporary use, without the permission of the copyright holder.

Counterfeiting means producing fake copies of a software, making it look authentic. This involves providing all designed to look as much like the original product as possible.

The fastest-growing form of piracy is Internet piracy. The exchange of software on the Internet has attracted an extensive following.

*5. Conclusion*

Some techniques for safe computing include keeping software patches and operating system service packs up to date, not opening suspicious e-mail attachments, obtaining software only from reliable resources and always scanning it for malware, avoiding unsavory Web sites.

Remember that many software programs exist and you can find usually alternatives with similar features offered under various licensing terms.

It is essential to use security software, but also important to take additional precautions, such as making regular backups of your data.