**1. What is computer virus?**

A virus is a piece of software designed and written to adversely affect your computer by altering the way it works without your knowledge or permission. In more technical terms, a virus is a segment of program code that implants itself to one of your executable files and spreads systematically from one file to another. Computer viruses do not spontaneously generate: They must be written and have a specific purpose. Usually a virus has two distinct functions:

* Spreads itself from one file to another without your input or knowledge. Technically, this is known as self-replication and propagation.
* Implements the symptom or damage planned by the perpetrator. This could include erasing a disk, corrupting your programs or just creating havoc on your computer. Technically, this is known as the virus payload, which can be benign or malignant at the whim of the virus creator.

A benign virus is one that is designed to do no real damage to your computer. For example, a virus that conceals itself until some predetermined date or time and then does nothing more than display some sort of message is considered benign.

A malignant virus is one that attempts to inflict malicious damage to your computer, although the damage may not be intentional. There are a significant number of viruses that cause damage due to poor programming and outright bugs in the viral code. A malicious virus might alter one or more of your programs so that it does not work, as it should. The infected program might terminate abnormally, write incorrect information into your documents. Or, the virus might alter the directory information on one of your system area. This might prevent the partition from mounting, or you might not be able to launch one or more programs, or programs might not be able to locate the documents you want to open.

Some of the viruses identified are benign; however, a high percentage of them are very malignant. Some of the more malignant viruses will erase your entire hard disk, or delete files.

### What Viruses Do

Some viruses are programmed specifically to damage the data on your computer by corrupting programs, deleting files, or erasing your entire hard disk. Many of the currently known Macintosh viruses are not designed to do any damage. However, because of bugs (programming errors) within the virus, an infected system may behave erratically.

### What Viruses Don't Do

Computer viruses don't infect files on write-protected disks and don't infect documents, except in the case of Word macro viruses, which infect only documents and templates written in Word 6.0 or higher. They don't infect compressed files either. However, applications within a compressed file could have been infected before they were compressed. Viruses also don't infect computer hardware, such as monitors or computer chips; they only infect software.

In addition, Macintosh viruses don't infect DOS-based computer software and vice versa. For example, the infamous Michelangelo virus does not infect Macintosh applications. Again, exceptions to this rule are the Word and Excel macro viruses, which infect spreadsheets, documents and templates, which can be opened by either Windows or Macintosh computers.

Finally, viruses don't necessarily let you know that they are there - even after they do something destructive. [[1]](#footnote-1)

## 2. Types of Computer Viruses

## Nowadays number of viruses is about 55000. It increases constantly. New unknown types of viruses appear. To classify them becomes more and more difficult. In common they can be divided by three basic signs: a place of situating, used operation system and work algorithms. For example according these three classifications virus Chernobyl can be classified as file infector and resident Windows virus. Further it will be explained what it means.

### 2.1 A place of existence

### 2.1.1File Infectors

These are viruses that attach themselves to (or replace) .COM and .EXE files, although in some cases they can infect files with extensions .SYS, .DRV, .BIN, .OVL and .OVY. With this type of virus, uninfected programs usually become infected when they are executed with the virus in memory. In other cases they are infected when they are opened (such as using the DOS DIR command) or the virus simply infects all of the files in the directory is run from (a direct infector).

There are three groups of file infectors.

Viruses of the **first group** are called overwriting viruses because they overwrite their code into infected file erasing contents. But these viruses are primitive and they can be found very quickly.

**Other group** is called parasitic or cavity viruses. Infected file is capable of work fully or partly but contents of last one are changed. Viruses can copy itself into begin, middle or end of a file. They record their code in data known not to be used.

**Third group** is called companion viruses. They don’t change files. They make double of infected file so when infected file is being started a double file becomes managing, it means virus. For example companion viruses working with DOS use that DOS firstly runs COM. file and after if this file is not found runs EXE. file. Viruses make double file with a same name and with extension COM and copies itself in this file. During start of infected file DOS runs a COM. file with a virus firstly and then a virus starts an EXE. file.

Sometime companion viruses rename file will be infected and record their code in a double file with old name. For example the file XCOPY.EXE is renamed into XCOPY.EXD and virus record itself in file XCOPY.EXE. When this file is started computer runs a virus code firstly and after virus starts original XCOPY, saved as XCOPY.EXD. Viruses like this were found not only in DOS. They were found in Windows and OS/2.

It is not only one way to make double files. For example there is subgroup of companion viruses called path-companion viruses. They use special feature of DOS - PATH: hierarchical record of file location. Virus copies itself in file with the same name but situated one level higher. In this case DOS will find file with virus. [[2]](#footnote-2)

### 2.1.2Boot viruses

### Boot Sector Infectors

Every logical drive, both hard disk and floppy, contains a boot sector. This is true even of disks that are not bootable. This boot sector contains specific information relating to the formatting of the disk, the data stored there and also contains a small program called the boot program (which loads the DOS system files). The boot program displays the familiar "Non-system Disk or Disk Error" message if the DOS system files are not present. It is also the program that gets infected by viruses. You get a boot sector virus by leaving an infected diskette in a drive and rebooting the machine. When the boot sector program is read and executed, the virus goes into memory and infects your hard drive. Remember, because every disk has a boot sector, it is possible (and common) to infect a machine from a data disk. NOTE: Both floppy diskettes and hard drives contain boot sectors.

### Master Boot Record Infectors

The first physical sector of every hard disk (Side Ш, Track Ш, Sector 1) contains the disk's Master Boot Record and Partition Table. The Master Boot Record has a small program within it called the Master Boot Program, which looks up the values in the partition table for the starting location of the bootable partition, and then tells the system to go there and execute any code it finds. Assuming your disk is set up properly, what it finds in that location (Side 1, Track Ш, Sector 1) is a valid boot sector. On floppy disks, these same viruses infect the boot sectors. You get a Master Boot Record virus in exactly the same manner you get a boot sector virus -- by leaving an infected diskette in a drive and rebooting the machine. When the boot sector program is read and executed, the virus goes into memory and infects the MBR of your hard drive. Again, because every disk has a boot sector, it is possible (and common) to infect a machine from a data disk. [[3]](#footnote-3)

### 2.1.3 Multi-partite Viruses

Multi-partite viruses are a combination of the viruses listed above. They will infect both files and MBRs or both files and boot sectors. These types of viruses are currently rare, but the number of cases is growing steadily.

**2.1.4 Macro Viruses**

Until recently, the macro languages included with most applications were not powerful or robust enough to support writing an effective virus. However, many of the more advanced applications that are being developed today include built-in programming capabilities that rival some of the larger development packages. This has recently been demonstrated by the various strains of Microsoft Word viruses, including the so-called Word Concept and Word Nuclear viruses. These viruses transport themselves through Microsoft Word documents. When opened in Word, they perform various actions, including spreading themselves into the user's installation of Word, thus preparing to infect all future documents on the system.

An additional concern is that macro viruses can be cross-platform. The Word Concept virus has the claim to fame of being the first prominent cross-platform virus, because it can infect both Windows and Macintosh systems.

Because most application macro languages support passing execution to an external shell, such as COMMAND.COM or CMD.EXE, the power of the macro virus is not limited to the constraints of the macro language itself[[4]](#footnote-4).

**2.2 Used operation system.**

Any computer or net virus can infect files of one or more operation systems: DOS, Windows, OS/2, Linux, MacOS and others. It is a base of this way of classification. For example virus BOZA working with Windows only is classified as Windows virus, virus BLISS – as Linux virus.

**2.3 Work algorithms.**

Viruses can be differed by used algorithms making them danger and hard for catching.

Firstly viruses can be divided on resident and nonresident.

Resident virus having come in operation memory of computer doesn’t infect memory. They are capable of copying when they are started only. We can call any macro virus resident. They present in memory during application infected by them works.

Second viruses are visible and invisible. To be invisible means that users and antivirus programs can’t notice changes of infected file done by virus. Invisible virus catches all requires of operation system to read file and to record in file and shows uninfected version of file. So we can see only ‘clear’ programs during virus works. One of first invisible file infectors was FRODO and boot infector – BRAIN.

Almost any virus uses methods of self-coding or polymorphism to escape antivirus programs. It means that they can change itself. Changing itself helps virus to be able work.[[5]](#footnote-5)

**3. Conclusion**

In conclusion I would like to say few words about future of this classification. Nowadays computer technologies and all software develop very quickly. It helps new types of computer viruses to appear. Viruses are becoming more and more dangerous and ‘cleverer’. It means that viruses can be found more and more hard. But I think that this classification can be saved a long time thank for principles of work of computer. It means that this classification will be changed when computers work by principles that differ from principles of von Neiman. So this classification can be change by adding new subtypes of basic types if virus makers have created something new.

Buryat State University

The paper: Types of computer viruses

Presented by Nefyodov Yuri

Scientific advisor: Sodboyeva L.D.

Ulan-Ude 2003

**Abstract**

This paper is about the classification of computer viruses. Firstly, the paper tells what a computer virus is, what viruses can do and what they can’t do. Then there are basic ways of classification: a place of situation, used operation system and work algorithms. In conclusion it’s said about future of classification.

**Аннотация**

Этот доклад посвящён классификации компьютерных вирусов. В начале рассказывается, что такое компьютерный вирус, что вирусы могут делать и что не могут. Далее здесь описаны три основных способа классификации: по среде обитания, используемой операционной системе и алгоритму работы. В заключении говорится о будущем классификации.

Plan

1. What is a computer virus?

2. Types of computer viruses.

2.1 a place of existence

2.1.1 file infectors

2.1.2 boot viruses

2.1.3 multi-partite viruses

2.1.4 macro viruses

2.2 used operation system

2.3 work algorithms

3. Conclusion.

References:

1. Могилёв, Хеннер, Пак «Информатика» Издательство «Академия» 2000г
2. Журнал «Наука и жизнь» №7 2000 год
3. сайт WWW.SEMANTEC.RU

1. WWW.SEMANTEC.RU [↑](#footnote-ref-1)
2. Наука и жизнь №7 2000 год стр. 100

   [↑](#footnote-ref-2)
3. Могилёв, Пак ,Хеннер Информатика 2000 изд. «Академия» [↑](#footnote-ref-3)
4. WWW.SEMANTEC.RU [↑](#footnote-ref-4)
5. Наука и жизнь №7 2000 год стр. 101-102 [↑](#footnote-ref-5)