SAFETY IN A NETWORK OF THE INTERNET

Fedorenko V.G.,*gr. FT-74*

Despite the huge means invested in the problem of computer safety, the quantity of safety in the networks connected to global network Internet grows. Both little-known sites and the whole networks of the large companies and the organizations are exposed to hacker attacks .

It occurs because of the infringement, if there no financial or political grounds and the motivation is connected with self-affirmation, thirst of knowledge or simply vandalism.

However, according to Defense Information Services Agency (DISA) 98 % of attacks remain unnoticed. For better safety no high qualification is required because of plenty of automatic means of infringement of safety. Owing to automation of means of attack, the qualification of the safety infringers goes down.

Now the majority of users are familiar with computer viruses and worms due to presence of destroying functions in them.. However it is necessary to note, that not destructive functions define a condition of technology of viruses creation because of the following:

- authors of original viruses seldom include destructive functions (they are added in most cases by unqualified hooligans);
- if your system is amazed by a virus, opportunities of infringement of information safety can vary.

From the above-stated reasons it follows that, speaking about a computer virus or a worm, it is necessary to consider the mechanism of infection and the mechanism of distribution.

Blossoming of viruses in their classical understanding has fallen to operational system MS DOS and occurred in 80s and in the early 90s. At that time viruses infected loading areas of stores on rigid and flexible disks and operation files. Viruses extended from a computer to a computer through the diskettes infected by viruses or containing infected files. During this period viruses have passed a way from the elementary viruses up to the coded ones. From the virus technologies developed during this period, it is necessary to note the following:

- «stealth» technology provided "invisibility" of viruses for standard means, delivering the information to the system;
- an orientation of some viruses to destruction or blocking of work of anti-virus programs in the amazed computer;

- development of generators of the viruses, which allowed unqualified users to create viruses automatically .

The Morris's worm is the best known worm. The virus appeared in 1988 and during a short time interval paralyzed work of many hosts of Internet network. This worm belongs to classical nocuous programs.

Morris's worm was a self-extending program which distributed the copies on the Internet, receiving exclusive access rights to hosts due to its "holes" in operational system. One of them, used by Morris's worm, was the vulnerable version of program Sendmail, and another of the program Fingerd. To defeat the systems the worm used also vulnerability of commands rexec and rsh, and also user passwords chosen incorrectly.

With the advent of family operational systems Windows in 90s the situation has changed.

In 1995 the virus Concept, the first macro-virus appeared. Since this moment the viruses infecting documents Microsoft Office became the most popular. After occurrence of the next version of product Microsoft Office in 1997, viruses have ceased to be specific to any separate office appendix, and became "general" for all products of the family, owing to the introduction of interpreted language Visual Basic.

Virus Melissa appeared in May, 1999 and amazed about 100000 hosts connected to the Internet, including the networks protected by gateway screens. The virus extended by means of the program attached to the post message. Even if in an attacked network there was a stock-taking of viruses at post messages, anti-virus means could not distinguish the signature of virus Melissa.

In January 1999 there appeared virus Caligula which extended by means of documents Microsoft Word / 97. The given virus tried to find out in the infected system a file containing the information, used by program PGP. Thus for communication with the infringer the session ftp, initiated with the infected machine was used. It allowed to bypass the gateway screen.

Thus, it is possible to ascertain, that the nocuous software, applying classical ideas, can use the opportunities which have been opened with the advent of new technologies.

Zolotova S.G. *EL adviser*