Julia Kolos
A.A. Baranov, research supervisor
M.L. Isakova, language adviser
SHEI “National Mining University”, Dnepropetrovsk

DDoS-attacks: How to Defeat the Avalanche?

Being one of the greatest evils of the Internet, the performance of DDoS-attacks is not too fast and not very easy deal with, but the consequences are heavy, and most importantly, they are very difficult to fight back. There is no reliable means of protection, but attempts to create them do not stop.

DDoS attack, Distributed attack, leads to a denial of access. Its essence lies in the fact that the hacker sends endless "junk" queries to one or more servers which causes the overload - and the denial of access. The victims of such attacks in 2000 became known resources Amazon.com, Yahoo!, eBay - and some more hugely popular sites. Potentially, any server is vulnerable. If it is not protected, then as the result of massive attack it is flooded or stop working.

It is possible to fight with DDoS attacks in the following ways:

- The most effective one is to put a firewall (also known as brandmauer), close all unnecessary ports and not to skip any transaction, except with the ports and applications that an administrator has prescribed in advance;
- You can manually block sources of "junk" traffic, but if there are a few thousand of these sources, it is unlikely to help;
- With traffic rate limitation you can ask the ISP to limit the volume of traffic. This type of filtering allows you to restrict the volume of uncritical traffic, transmitted at your network. For example, there is the limitation the volume of traffic ICMP, which is only used for target diagnostic. DDoS attacks often use ICMP.
- FloodGuard (software and hardware system). Working principle of this system looks as follows. Detectors are installed on firewalls, switches and routers, which constantly monitor traffic and create its "profile" (or "mask"), based on such characteristics as the volume of data packets, their type, source, direction and so on. In case of appearance of any anomaly detector tells the executive modules (actuators), sending them the information about these anomalies, about source of the attack, the volume of parasitic traffic and type of packets. Executive modules located on routers in different network segments constantly monitor the traffic as well, and to obtain data about the appearance of parasitic packets, start to find them in the data that passes through them. If the parasitic packets are detected, the executive module immediately sends an alarm to the previous module, with recommendations to activate the filters on the relevant routers.

Thus, the avalanche of "junk" data erected a barrier, and besides is blocked not everything, namely malicious traffic. Barrier can be erected in automatic mode, but there is the opportunity of manual settings.