Alexandr Bublik
A.V. Gerasina, research supervisor
V.V. Gubkina, language adviser
SHEI “National Mining University”, Dnipropetrovsk

Intrusion Prevention and Intrusion Detection Systems

The time goes by and we constantly observe the rapid development in information technology area. Nowadays it becomes clear that protecting information is getting harder and harder. It is obviously, that the threat of attacks on corporate systems is more than real. But whether companies would be able to protect themselves from the complex and elaborate attacks?

That is the main point of the fact that lots of companies use Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS). It's important to start out with the understanding that IDS and IPS are very, very different tools. Even though they have a common base, they fit into the network in different places, have different functions, and solve different problems.

An Intrusion Detection System (IDS) is designed to monitor all inbound and outbound network activity and identify any suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. It is worth noting that this information protection technology had been using for a long time and became quite popular among customers. IDS specifically looks for any events that might be the result of a virus, worm or hacker. A good analogy is to compare IDS with a protocol analyzer, that a network engineer uses to look deep into the network and see what is happening, in sometimes infinitesimal detail. So, IDS carries out an analysis of the network and sees every action from the security point of view. With regard to IPS or intrusion prevention system, it is definitely the next level of security technology with its capability to provide security at all system levels. Where IDS informs of a potential attack, IPS makes attempts to stop it. Another huge progress over IDS, is that IPS has the capability of being able to prevent known intrusion signatures, but also some unknown attacks due to its database. So we can conclude that if IDS is a visibility tool, then IPS is a control tool. But they are not designed to meet the specific needs of internal security. For instance, neither can secure the internal network from the destructive spread of worms when you connect laptops directly to the internal network. Also the attack protection capabilities of these systems are limited to the specific devices on which the products are installed. Besides, highly qualified experts find IDS and IPS one of the effective and reliable ways to deal with hackers.