Vladyslav Hryhorenko
V.I.Mieshkov, research supervisor,
V.V.Gubkina, language adviser,
National Mining University, Dnipro, Ukraine

Linux Security

Information age has brought a new colossal change in a person's habitual life. The level of computer literacy has grown greatly and even a middle level specialist is able to perform the tasks intended for the programming experts. Computers integrated into the network provide a huge amount of confidential and sensitive information that has an impact on individuals as well as on the economies of enterprises or even affects the whole country.

With the constant growth of such information the need to secure it is growing as this increases the number and severity of cybercrimes. Based on this, we can conclude that information is a very valuable thing and requires been protected. Usually a key role is assigned to the staff. Automation and advanced level of engineering and technical skills resulted in a high level of computer literacy giving ordinary users not being qualified specialists in this field the possibility to perform different processing activities with the help of computers. To ensure a sufficient level of information security, evaluating the level and awareness of the staff as well as assessing appropriate software to meet high requirements is greatly recommended.

In conditions of severe competition and low costs of licensed software applications, Linux takes its special place. The area of applying a free operating system is very wide starting from the creation of special effects to the launch of space shuttles. Being free and secure Linux is turned into a really good tool meeting the high demands ranging from average users to great international companies.

So, what features make this operational system so popular? The answer lies in its simplicity. The user's work initially includes an "unprivileged" user. Setting "administrator" mode is available only for system configuration etc. An ordinary user is only entitled to read system files without possibility to change or make any harmful actions. Linux has different system to provide access rights. It does not have a familiar registry where all programs have a single address and unprivileged user has the right only to read. In the case of running a malicious program that can delete all the sensitive data, only user's directory will be under the attack while system folders will not be affected. Users are given high competence to improve a system view. Any program cannot be automatically turned on, thus making this feature a very significant one for a system operation.

It should be noted that neither operating systems nor firewall or antivirus could provide full security in the case of not following to simple security rules and requirements. Nowadays, the levels of software security and possible threats are approximately at the same point. A great fortune of money is allocated for developing and enhancing security systems. Using key features and following the main Linux security rules you can be sure of your safety.