Vasilisa Holoborodko
V.I. Mieshkov, research supervisor
S.I. Kostrytska, language adviser
National TU «Dnipro Polytechnic», Dnipro, Ukraine

Social Engineering in Information Security

People are very focused on the new computer attack techniques. They forget about the “human attacks”. Social engineering is a method of unauthorized access to information or to the storage systems without technical means. The term has been determined recently. However, the method has been used for a long time.

The main goal of social engineering is getting access to the confidential information, passwords, bank data and another protected systems.

All techniques of social engineering are based on cognitive distortions. The main techniques of social engineering are fishing (stealing user confidential information), phreaking (hacking phone systems by manipulation with tone set), pretexting (using the prepared plan to make the victim to divulge information), getting information from open sources (gathering information from open sources as social networks), shoulder surfing (getting the victim personal information over his shoulder), and reverse social engineering.

Some social engineering experts separate the reverse and direct social engineering. The former is a method to organize the situation when a victim asks a malefactor for help.

In the classification of threats from social engineers the following threats can be determined: phone threats, e-mail threats, instant messaging threats.

The main way to protect users from social engineering is training. So, forewarned is forearmed. Ignorance of the law is no excuse. All employees must know the danger of disclosing information, and the methods that can prevent it.

Besides, the employees must have clear instructions as for the themes they can talk about, and what information for exact authorization they need to get from interlocutor.

There are no common rules to counteract the social engineers, because it is impossible to be protected from all techniques of the method. However it is possible to reduce the success of the method thanks to working out the appropriate policy of data classification; protecting information about clients with data encryption or using access control; training the employees the skills they need to identify the social engineer, to suspect those people, who are not familiar; forbidding the employees to exchange the passwords or to use the common ones; forbidding to give information with secrets to person, who is not familiar or not authorized in any way; using the special verification procedures for all who have requested access to the confidential information and testing the security system.