Sergey Mamienko
V.I. Mieshkov, research supervisor
I.I.Zuyenok, language adviser
National Mining University, Dnipro, Ukraine

# Smartphone security

According to eMarketer researchers, the total number of smartphones in active use on the planet exceeded the 2 billion unit in 2016 and amounted up to 2.16 billion against 1.9 billion in 2015 and 1.6 billion devices in 2014. A lot of owners of smartphones think that their communication, data exchange and privacy through their mobile or iPhones are completely protected from hacking and steeling as well as listening to, though they even can't imagine that his or her phone has been hacked or their personal information has been sent to a cybercriminal. The main ways of possible hacking the information and tips how to provide safety of the information contained in smartphones are in the focus of this paper. The usual method of hacking a smartphone is launching a malicious program through an application or link sent from unreliable and/or unknown source. Malicious programs fall into three main categories: viruses, trojans, and spyware. Most of the Trojans for smartphones are engaged in recording conversations or receiving instant messages, registering your location using GPS or giving outsiders the details of calls and/or other private information. Any spyware can collect information about users, who are not aware and have no idea of this action. Free access points to Wi-Fi are another way of collecting personal data or transferring malware. If a free Wi-Fi in a public place is not provided by a reputable Wi-Fi providers , it should be avoided to use.

Also, the personal information can be also stolen by a cybercriminals, especially in cases, when a smartphone has been stolen.

The following tips could be recommended for providing extra security for personal smartphones:

1. Set the password to lock the screen and use a special program to set passwords for all the applications that have important data.
2. Avoid using non-secure access points. Ii is more secure and reliable to use the own portable wireless access point, instead.
3. Download apps for your smartphone only from the official sources and known markets.
4. Regularly use antivirus program to scan a phone and its applications.
5. Always check and update the software and applications. Because companies that release software or applications sometimes find errors in the security of the program and with the help of updates eliminate them.

To sum up, an owner of a smartphone should be aware of the possible unsanctioned access to their personal data and take additional measures to provide the additional security of their phones.